UNIVERSIDAD DE MÁLAGA
ESCUELA POLITÉCNICA SUPERIOR
DEPARTAMENTO DE MATEMÁTICA APLICADA

La ecuación de Legendre $ax^2 + by^2 + cz^2 = 0$ en los Enteros de Gauss y en el Anillo de Polinomios Racionales

JOSÉ LUIS LEAL RUPERTO

TESIS DOCTORAL

Noviembre de 2015

AUTOR: José Luis Leal Ruperto

http://orcid.org/0000-0002-9487-6016

EDITA: Publicaciones y Divulgación Científica. Universidad de Málaga

Dr. Juan José Saameño Rodriguez, Titular de Universidad del Departamento de Matemática Aplicada de la Universidad de Málaga,

hace constar:

Que D. José Luis Leal Ruperto, Licenciado en Ciencias Matemáticas, ha realizado en el Departamento de Matemática Aplicada de la Universidad de Málaga, bajo mi dirección, el trabajo de investigación correspondiente a su Tesis Doctoral titulado:

La ecuación de Legendre en los Enteros de Gauss y en el Anillo de los Polinomios Racionales

Revisado el presente trabajo, estimo que puede ser presentado al tribunal que lo ha de juzgar. Y para que conste a efectos de lo establecido en el Real Decreto 185/1985, autorizo la presentación de este trabajo en la Universidad de Málaga.

Málaga, de Octubre de 2015

Juan José Saameño Rodriguez

A la memoria de mi hija Miranda

Agradezco a mi mujer Valeria por su paciencia estos tres años, también a los compañeros del departamento que con su ejemplo me han motivado en el deseo de investigar, Iván Atencia que me ha ayudado no solo con el inglés, Emilio Muñoz por su actitud siempre positiva, Inmaculada de las Peñas por haberme picado hace ya muchos años a que le dedicara tiempo a una tesis, a Luis Lechuga su interés por escucharme estos años y hacerme observaciones, a Antonio Garvín por sus continuas preguntas acerca de como iba en mi investigación, a Cristina Drapper y Francisco Palomo por darle valor a mi esfuerzo y a mi compañero y director de Tesis Juan José Saameño.

Quiero dedicar este trabajo a los profesores Francisco Luis Cardosa Urda, Inmaculada Pérez de Guzmán Molina, Amín Kaidi y Florencio del Castillo Abánades, profesores que, de entre los que tuve, me enseñaron Matemáticas.

Prefacio

La motivación que ha dado lugar a esta tesis surgió en clase. Estos últimos años había tratado con más detalle la geometría analítica en $\mathbb{R}^3$, con objeto de que los alumnos de Ingeniería de las especialidades de Diseño Industrial y Mecánica tuvieran un mejor dominio del espacio.

En particular explico con más detalle y más ejemplos las transformaciones ortogonales o isometrías y los movimientos, que son importantes en cualquier modelo que ellos pudieran implementar en dos o tres dimensiones.

Las matrices que representan estas transformaciones y movimientos son matrices ortogonales en las que tanto las filas como las columnas son vectores perpendiculares dos a dos y unitarios. Por ejemplo en $\mathbb{R}^2$ lo es la siguiente matriz de valores racionales,

$$\begin{pmatrix} \frac{15}{17} & \frac{8}{17} \\ \frac{8}{17} & -\frac{15}{17} \end{pmatrix}.$$

La dificultad al proponer ejercicios simples en clase sobre giros, reflexiones y otros movimientos está siempre en seleccionar bases ortonormales con entradas racionales. El proceso de Gram Schmidt no lo garantiza y cuando se efectúan las operaciones de cambio de base para calcular la matriz de la transformación respecto a la base canónica, arrastramos números con raices cuadradas no exactas, números de expresión complicada para manejarlos por parte del alumno en un primer estudio.

Para hallar una base ortonormal de valores racionales, primero hay que buscar vectores racionales que sean unitarios, en $\mathbb{R}^2$ equivale a la búsqueda de soluciones enteras de

$$x^2 + y^2 = z^2,$$

ya que x_o, y_o, z_o es solución entera de la ecuación anterior si y sólo si $(\frac{x_o}{z_o}, \frac{y_o}{z_o})$ es vector unitario de $\mathbb{R}^2$. Las soluciones de esta ecuación son conocidas como

las **ternas pitagóricas**. La terna asociada a la matriz ortogonal anterior es $(15, 8, 17)$.

En la mayor parte de textos elementales de teoría de números se presenta una fórmula para la parametrizacón de las ternas con X, Y enteros,

$$\begin{aligned} x &= X^2 - Y^2 \\ y &= 2XY \\ z &= X^2 + Y^2 \end{aligned} \tag{1}$$

y con una demostración directa de la validez de las mismas.

En $\mathbb{R}^2$, el conocimiento de cualquier vector unitario $\vec{v} = (a_{11}, a_{12})$ automaticamente genera las posibles matrices ortogonales que lo contienen en alguna fila o columna. Sólo pueden ser

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{12} & -a_{11} \end{pmatrix},$$

y las que resultan cambiando los signos de los vectores o permutando a_{11} con a_{12}.

En $\mathbb{R}^3$, los vectores unitarios se obtienen de las soluciones enteras de

$$x^2 + y^2 + z^2 = t^2, \tag{2}$$

o **cuaternas pitagóricas**. Pero como vemos en este ejemplo de matriz ortogonal racional,

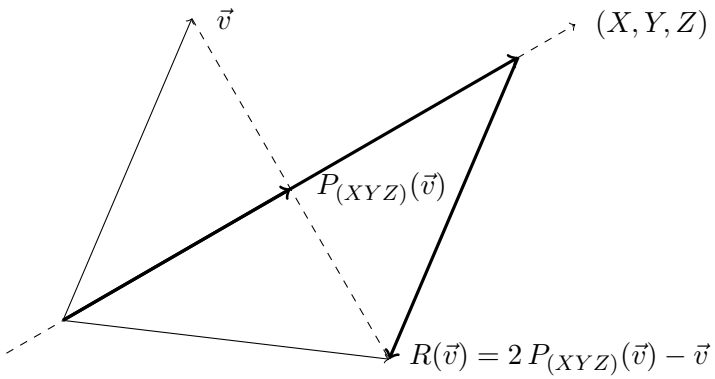
$$\frac{1}{15}\begin{pmatrix} 11 & -10 & 2 \\ 2 & 5 & 14 \\ 10 & 10 & -5 \end{pmatrix},$$

disponer de una cuaterna como $11, 2, 10, 15$ no da la información necesaria de todas las matrices ortogonales que la contienen.

En el transcurso del cálculo en clase de la matriz en la base canónica de la reflexión sobre un vector en $\mathbb{R}^3$ de dirección (X, Y, Z), en la que decidí hacer uso de la fórmula, que había observado que era geométricamente cierta:

$$R(\vec{v}) = 2\, P_{(X,Y,Z)}(\vec{v}) - \vec{v}$$

es decir, la reflexión de un vector $\vec{v}$ respecto a un vector de dirección (X, Y, Z) es dos veces la proyección de $\vec{v}$ sobre la dirección de ese vector menos $\vec{v}$, como puede verse en el dibujo,



noté que al hacer la reflexión de los vectores canónicos $(1,0,0)$, $(0,1,0)$ y $(0,0,1)$ que son de norma 1, obtenidos de las que son soluciones de $x^2 + y^2 + z^2 = t^2$, respectivamente $(1,0,0,1)$, $(0,1,0,1)$ y $(0,0,1,1)$, que por la naturaleza de la fórmula en el que se suman, multiplican y dividen racionales, se obtenía directamente la matriz ortogonal con entradas racionales.

En $\mathbb{R}^2$ la reflexión del vector unitario $(1,0)$ proveniente de la solución $(1,0,1)$ respecto a la dirección (X,Y), con X e Y parámetros enteros da

$$\begin{aligned} R(1,0) =& 2\frac{(1,0)(X,Y)^t}{(X,Y)(X,Y)^t}(X,Y) - (1,0) = \\ =& \left(\frac{X^2 - Y^2}{X^2 + Y^2}, \frac{2XY}{X^2 + Y^2}\right), \end{aligned}$$

extrayendo los valores de los numeradores y el denominador, obtenemos las mismas fórmulas que en (1).

En $\mathbb{R}^3$ la reflexón de $(1,0,0)$ proveniente de la solución $(1,0,0,1)$ respecto a (X,Y,Z),

$$\begin{aligned} R(1,0,0) =& 2\frac{(1,0,0)(X,Y,Z)^t}{(X,Y,Z)(X,Y,Z)^t}(X,Y,Z) - (1,0,0) = \\ =& \left(\frac{X^2 - Y^2 - Z^2}{X^2 + Y^2 + Z^2}, \frac{2XY}{X^2 + Y^2 + Z^2}, \frac{2XZ}{X^2 + Y^2 + Z^2}\right) \end{aligned}$$

nos proporciona también de forma inmediata una parametrización de (2).

$$\begin{aligned} x &= X^2 - Y^2 - Z^2 \\ y &= 2XY \\ z &= 2XZ \\ t &= X^2 + Y^2 + Z^2. \end{aligned}$$

Esta parametrización ya no es fácil verla en los libros, porque su prueba directa es compleja y no es generalización del caso $n = 2$. Hay numerosos artículos acerca de las cuaternas pitagóricas, incluso recientes, en donde de distintas formas, con más o menos dificultad se llega a encontrar y probar una parametrización de todas las soluciones. (Ver por ejemplo [17], [28] y sus bibliografías).

Haciendo la reflexión con el resto de los vectores canónicos se tiene la matriz ortogonal de entradas racionales,

$$\begin{pmatrix} X^2 - Y^2 - Z^2 & 2XY & 2XZ \\ 2XY & -X^2 + Y^2 - Z^2 & 2YZ \\ 2XZ & 2YZ & -X^2 - Y^2 + Z^2 \end{pmatrix}$$

matriz simétrica, que no es una parametrización completa de todas las ortogonales racionales porque éstas, sólo corresponden a la reflexión respecto a un vector, o giro de 180 grados. En $\mathbb{R}^3$ existen otras isometrías, como los giros y composición de giro y simetría respecto a un plano, y todas ellas son también representadas por matrices ortogonales [1].

[1] Una parametrización completa se obtiene del hecho de que existe una correspondencia uno a uno entre el conjunto de las matrices hemisimétricas racionales y el conjunto de matrices ortogonales racionales (ver [22]) dada por

$$H \to (H - I)^{-1}(H + I),$$

con I identidad. Por ejemplo en $\mathbb{R}^3$ cualquier hemisimétrica es del tipo

$$\begin{pmatrix} 0 & X & Y \\ -X & 0 & Z \\ -Y & -Z & 0 \end{pmatrix}$$

que se transforma de acuerdo con la correspondencia, en

$$\begin{pmatrix} \frac{-Z^2+Y^2+X^2-1}{Z^2+Y^2+X^2+1} & \frac{2YZ-2X}{Z^2+Y^2+X^2+1} & \frac{-2XZ-2Y}{Z^2+Y^2+X^2+1} \\ \frac{2YZ+2X}{Z^2+Y^2+X^2+1} & \frac{Z^2-Y^2+X^2-1}{Z^2+Y^2+X^2+1} & \frac{2XY-2Z}{Z^2+Y^2+X^2+1} \\ \frac{2Y-2XZ}{Z^2+Y^2+X^2+1} & \frac{2Z+2XY}{Z^2+Y^2+X^2+1} & \frac{Z^2+Y^2-X^2-1}{Z^2+Y^2+X^2+1} \end{pmatrix}$$

El procedimiento geométrico es generalizable en $\mathbb{R}^n$ con la solución

$$1, 0, 0, \cdots, 0, 1$$

de la ecuación $x_1^2 + x_2^2 + \cdots + x_n^2 = x_{n+1}^2$.

El haber llegado a las parametrizaciones por esta via, que no he visto que se hiciera o se mencionara en ninguna parte, me hizo interesarme por la ecuación más general,

$$ax^2 + by^2 + cz^2 = 0,$$

de la que yo nada sabía, y de la que obtuve, generalizando el procedimiento anterior, conocida una solución (x_o, y_o, z_o), que juega ahora el mismo papel que la solución (1,0,1), una parametrización de todas las demás soluciones, con dos parámetros enteros X, Y:

$$\begin{aligned} x = &\quad ax_oX^2 + 2by_oXY - bx_oY^2 \\ y = &-ay_oX^2 + 2ax_oXY + by_oY^2 \\ z = &\quad z_o(aX^2 + bY^2). \end{aligned}$$

Resultó ser una ecuación clásica de la que desde Diofanto en su tomo II, articulo 20, y desde la época 1767 con Lagrange, había sido investigada con interés y esfuerzo por numerosos matemáticos. Dickson [8] en su *History of the Theory of Numbers. Volume II. Diophantine Analysis*, de 1919 le dedica una sección, en la que hay numerosas referencias acerca de cómo enfocaron el problema de la resolubilidad de la ecuación y del cálculo en paramétricas de las soluciones.

Existen ecuaciones que tienen solución y otras que no. Para las que la tienen nadie usó con anterioridad el sencillo enfoque geométrico antes expuesto, cosa que me sorprendió a la vez que me motivó y animó a la vista de los complicados prodedimientos para hallar soluciones, y no todas, a los que llegaban.

No es hasta Réalis [7] en 1878 cuando se expone, sin probar que representan a todas las soluciones, unas fórmulas explicitas de las soluciones en función de tres parámetros enteros.

El interés por esta ecuación y de las ecuaciones homogéneas cuadráticas en general con n variables parece decrecer con el desarrollo en el pasado siglo

que es ortogonal y dependiente de $\frac{1}{2}(3^2 - 3) = 3$ parámetros racionales, equivalente a 4 parámetros enteros.

En el caso n dimensional, la matriz ortogonal depende de $\frac{1}{2}(n^2 - n) + 1$ parámetros enteros.

de los p-ádicos, al probarse que las ecuaciones cuadráticas y en particular la ecuación $ax^2 + by^2 + cz^2 = 0$ de Legendre puede resolverse p-ádicamente, por las técnicas llamadas locales-globales:

La ecuación $ax^2 + by^2 = cz^2$ tiene soluciones enteras primitivas si y sólo si tiene soluciones reales y soluciones enteras primitivas módulo n para todo $n \geq 2$.

Las ecuaciones que tienen este comportamiento se dice que satisfacen el principio de Hasse. En particular para la ecuación $ax^2 + by^2 + cz^2 = 0$ se prueba [21] que es resoluble si y sólo si tiene soluciones en $\mathbb{R}$, y las tiene módulo cada divisor de $2abc$.

Pero no se ha probado que la ecuación es p-ádica resoluble en un dominio euclídeo $\mathbb{E}$ diferente al de $\mathbb{Z}$, por lo que por esta vía, parece que no puede pensarse en buscar generalizaciones.

He visto que la generalización de lo que se conoce acerca de la ecuación de Legendre en otros dominios euclídeos puede hacerse desde los argumentos originales de Legendre. Samet [15] resuelve el teorema de Legendre en los enteros de Gauss. Hemer lo resuelve [16] en otros dominios euclídeos cuadráticos imaginarios, ambos en los años 50, pero desde entonces y hasta ahora, salvo la prueba reciente [26] del teorema de legendre en el dominio euclídeo $\mathbb{Z}[\omega]$, con $\omega = \frac{-1+\sqrt{-3}}{2}$ raíz de la ecuación $x^2 + x + 1 = 0$, no se había probado nada más.

Investigaciones actuales sobre ecuaciones cuadráticas en general, lo que estudian es el problema de determinar, caso de ser resoluble, si existe una solución que pueda considerarse minimal, o la de establecer una cotas acerca de la posible magnitud de una solución.

Holzer [12] establece dichas cotas para la ecuación de Legendre en $\mathbb{Z}$, probando que si la ecuación $ax^2 + by^2 + cz^2 = 0$ es resoluble, existe entonces una solución (x, y, z) con $|x| < \sqrt{|bc|}$, $|y| < \sqrt{|ac|}$, $|z| < \sqrt{|ab|}$.

En [24] en la ecuación más general $a_1x_1^2 + a_2x_2^2 + \cdots + a_nx_n^2 = 0$, que existe una solución con $|a_1|x_1^2 + |a_2|x_2^2 + \cdots + |a_n|x_n^2 \leq 2|a_1a_2 \cdots a_n|$, y en [27] se estudian esas cotas en ciertos casos particulares.

Recuperando el enfoque original de Legendre, en esta tesis resuelvo lo siguiente:

1. En el capítulo 6 generalizo el teorema de Holzer para la ecuación de Legendre en los Enteros de Gauss $\mathbb{Z}[i]$. Publicado [29].

2. En el capítulo 7 resuelvo la ecuación de Legendre en el anillo de los polinomios racionales $\mathbb{Q}[t]$. Aceptado en revisión [30].

3. En el capítulo 8 generalizo el teorema de Holzer en el anillo de polinomios racionales $\mathbb{Q}[t]$. Enviado para su posible publicación [31].

4. En el capítulo 9 resuelvo cuándo la ecuación de Legendre, en el anillo de los polinomios racionales $\mathbb{Q}[t]$, tiene solucion entera, y caso de tenerla, el procedimiento para calcular la única que existe. En el momento presente lo estoy redactando en detalle para ser enviado para su posible publicación.

Previamente, en el capítulo 1, una introducción con un poco de historia y con las cuestiones previas que son necesarias para tener una idea global de los trabajos de Lagrange y Legendre y Holzer en $\mathbb{Z}$. Las nuevas aportaciones en ello se sustentan.

Al final de ese capítulo primero expongo con detalle los teoremas que he probado.

En el capítulo 2, entramos en detalles. Incluyo lo que es necesario, algunas cosas son elementales, pero no por ello se está familiarizado con ellas. Se termina en 2.3.1 con la prueba del teorema de Legendre en $\mathbb{Z}$ que hace Dirichlet [6]. Una genial demostración por inducción sobre el Índice de la ecuación, que disipa las dudas que planteó Gauss [4] acerca de la demostración "con puntos suspensivos" que hizo legendre [2]. Esta demostración será la base de la generalización a $\mathbb{Z}[i]$ y $\mathbb{Q}[t]$.

En el capítulo 3, se explican las distintas parametrizaciones que se conocen acerca de las soluciones. En 3.3 incluyo el procedimiento generalizado de la reflexión antes descrito para la ecuación de legendre. También resuelvo el problema inverso de encontrar las ecuaciónes que satisfacen cierta solución.

En el capítulo 4, se hace la prueba del teorema de Holzer en los enteros que hizo Mordell [18], demostración que a diferencia de la original de Holzer, si permite ser generalizada en $\mathbb{Z}[i]$ y $\mathbb{Q}[t]$.

El capítulo 5, se dedica a los enteros de Gauss, donde resumimos los fundamentos de ese dominio euclídeo para poder exponer en 5.4 la demostración original de Samet [15], con detalle, del teorema de Legendre en $\mathbb{Z}[i]$.

En el capítulo 10, aporto algunas ideas de posibles generalizaciones de los resultados a otros deminios euclídeos, y de otros problemas relacionados que se cuestionan, no resueltos hasta ahora.

Málaga Septiembre de 2015.

Índice

1

Introducción

Desde Lagrange [1], ya era conocido que el problema de la resolubilidad en los enteros de la ecuación cuadrática homogénea ternaria,

$$ax^2 + bxy + cy^2 + dxz + eyz + fz^2 = 0, \tag{1.1}$$

con coeficientes enteros, era equivalente al de la resolubilidad de la ecuación

$$x^2 - By^2 = Az^2, \tag{1.2}$$

en donde A, B son ambos enteros positivos y sin factores que sean cuadrados. Esta última ecuación se obtenía después de que se hiciera en las indeterminadas de (1.1) una transformación lineal o transformada [1]. De éstas, se sabía que existen ecuaciones con solución y otras sin solución salvo la trivial $(0, 0, 0)$ que siempre lo es.

Al tratarse de una ecuación homogénea, si x_o, y_o, z_o es solución de (1.2) también lo es cualquier múltiplo. Una solución es **primitiva** si el máximo común divisor (x_o, y_o, z_0)=1.

Con elementales argumentos sobre divisibilidad puede probarse que por ejemplo la ecuación,

$$x^2 - 5y^2 = 3z^2,$$

no tiene soluciones: Supongamos que (x_o, y_o, z_o) es solución primitiva no trivial. Es evidente que ninguno de x_o, y_o, z_o puede ser cero. Entonces como $[-5]_3 = [1]_3$, se tiene

$$[x_o - 5y_o^2]_3 = [x_o^2 + y_o^2]_3 = [0]_3,$$

[1] Las indeterminadas ya transformadas de $x^2 - By^2 = Az^2$ están renombradas de nuevo con x, y, z.

pero esto es sólo posible si $[x_o]_3 = [y_o]_3 = [0]_3$, que implica $[x_o^2]_9 = [y_o^2]_9 = [0]_9$, y que $[3z_o^2]_9 = [0]_9$. Luego también z_o^2 y en consecuencia z_o son múltiplos de 3 lo que es contradicción porque hemos supuesto que la solución es primitiva.

Para esta otra ecuación, por ejemplo $x^2 - 7y^2 = 2z^2$, es fácil ver que $(3, 1, 1)$ es solución, pero también lo serán las infinitas ternas,

$$(3X^2 - 14XY + 21Y^2, -X^2 + 6XY - 7Y^2, X^2 - 7Y^2)$$

cualesquiera que sean X, Y enteros. Estas fórmulas se obtienen con la ayuda de la solución particular conocida, y todas ellas pueden ser parametrizadas con al menos dos parámetros enteros, en el capítulo 3 veremos como.

Lagrange observa que existen condiciones que son a priori necesarias para la resolubilidad de $x^2 - By^2 = Az^2$. Supongamos que una ecuación tiene solución (x_o, y_o, z_o), supongamosla primitiva. Tenemos entonces que siempre será cierto,

Lema 1.1 *Si x_o, y_o, z_o es solución primitiva de $x^2 - By^2 = Az^2$, con A, B libres de cuadrados, entonces y_o es inversible en $\mathbb{Z}_A$.*

Observemos primero, que siempre,

$$(x_o, y_o) = (x_o, z_o) = (y_o, z_o) = 1,$$

ya que si fuese $(x_o, y_o) \neq 1$ tendríamos $x_o = px'$, $y_o = py'$ con p primo común con $p^2x'^2 - Ap^2y'^2 = Bz_o^2$, y entonces $[Bz_o^2]_{p^2} = [p^2]_{p^2}[x'^2 - Ay'^2]_{p^2} = [0]_{p^2}$, pero esto no es posible porque p no divide a z_o y p^2 no divide a z_o^2, y tampoco p^2 divide a B que está libre de cuadrados.

y también siempre,

$$(y_o, A) = 1,$$

ya que si p fuera primo común tendríamos $y_o = py'$, $A = pA'$, $x_o^2 = p(Bpy'^2 + A'z_o^2)$ y p dividiría también a x_o lo que no es posible por ser $(x_o, y_o) = 1$. Por tanto y_o es inversible en Z_A, el lema está probado.

Siendo así, podemos multiplicar entonces por el cuadrado del inverso de y_o a $[x_o^2 - By_o^2]_A = [0]_A$, y obtenemos $[(x_o/y_o)^2 - B]_A = [0]_A$, es decir,

$$[(x_o/y_o)^2]_A = [B]_A. \tag{1.3}$$

Permutando A y B también es cierto que

$$[(y_o/x_o)^2]_B = [A]_B. \tag{1.4}$$

Cuando, como en este caso, un entero B coincide con un cuadrado módulo otro entero A se dice que es residuo cuadrático:

Definición 1.1 *B es residuo cuadrático módulo A si existe un entero α tal que*

$$[\alpha^2]_A = [B]_A.$$

Es decir $\alpha^2 - B = AM$ para cierto M.

Por lo tanto, como concluimos en (1.3) y (1.4) que B es residuo cuadrático módulo A, y que A es resíduo cuadrático de B podemos afirmar:

Lema 1.2 (Condicion necesaria para $x^2 - By^2 = Az^2$, Lagrange) *La ecuación*

$$x^2 - By^2 = Az^2,$$

con A, B libre de cuadrados, si tiene solución, entonces es condición necesaria que B sea residuo cuadrático módulo A, y que A sea residuo cuadrático módulo B.

Partiendo de una ecuación que satisface la condición necesaria, Lagrange idea un procedimiento para resolverla conocido como **el método del descenso**. Este método consiste en la realización de un número finito de sucesivas **transformadas**[2], con la progresiva reducción del módulo de los coeficientes de las ecuaciones transformadas, y con las soluciones de todas ellas en correspondencia uno a uno. La solución general de la ecuación $x^2 - By^2 = Az^2$, se obtendría entonces a partir de la solución de la última y de todas las transformadas que le preceden.

Para hacer la primera transformada, y de la misma forma las que le siguen, Lagrange hace lo siguiente:

Supone $B < A$. Como existe un entero α tal que

$$[\alpha^2]_A = [B]_A, \tag{1.5}$$

elijamoslo de manera que $|\alpha| \leq \frac{1}{2}|A|$.

[2]Transformaciones lineales en las variables.

Si fuese mayor que la mitad, bastaría tomar $\alpha - A$, que en valor absoluto, si es menor que la mitad de A.

Para cierto M, tendremos entonces

$$\alpha^2 - B = AM, \qquad |\alpha| \leq \frac{1}{2}|A|. \tag{1.6}$$

Factorizemos,

$$M = A'k^2 \tag{1.7}$$

siendo k^2 el mayor cuadrado que divide a M, y la primera transformada es,

$$X^2 - BY^2 = A'X^2, \tag{1.8}$$

en la que A' está libre de cuadrados y el módulo $|A'|$ se ha reducido respecto a $|A|$ ya que,

$$|A'| \leq |M| = \left|\frac{\alpha^2 - B}{A}\right| \leq \left|\frac{\alpha^2}{A}\right| + \left|\frac{B}{A}\right| \leq \frac{1}{4}|A| + 1 < |A|. \tag{1.9}$$

Siempre $|A|$ puede considerarse que es mayor que 1, de otro modo la ecuación inicial (1.2) sería $x^2 - y^2 = z^2$ que tiene solución (1,1,0).

En esta nueva ecuación, si (X_o, Y_o, Z_o) es una solución, lo es (x_o, y_o, z_o) de $x^2 - By^2 = Az^2$ con

$$\begin{aligned} x_o &= \alpha X_o + BY_o \\ y_o &= X_o + \alpha Y_o \\ z_o &= A'kZ_o, \end{aligned}$$

obtenida mediante transformación lineal no singular.

Volviendo a reducir esta última y las que resultan de forma sucesiva, obtenemos una sucesión de transformadas [3],

$$\begin{aligned} x^2 - By^2 &= Az^2 && B < A \\ x^2 - By^2 &= A'z^2 && B < A' < A \\ x^2 - By^2 &= A'_1 z^2 && B < A'_1 < A' \\ \cdots &= \cdots \\ x^2 - By^2 &= A'_n z^2 && A'_n < B < A'_{n-1} \end{aligned} \tag{1.10}$$

[3] Renombramos siempre las sucesivas indeterminadas con x, y, z para simplificar la notación.

renombrando $B_1 := A'_n$ y $A'' := B$,

$$\begin{aligned}
x^2 - B_1y^2 &= A''z^2 \\
x^2 - B_1y^2 &= A''_1z^2 && B_1 < A''_1 < A'' \\
x^2 - B_1y^2 &= A''_2z^2 && B_1 < A''_2 < A''_1 \\
\cdots &= \cdots \\
x^2 - B_1y^2 &= A''_mz^2 && A''_m < B_1 < A''_{m-1}
\end{aligned}$$

renombrando $B_2 := A''_m$ y $A''' := B_1$,

$$\begin{aligned}
x^2 - B_2y^2 &= A'''z^2 \\
\cdots &= \cdots \\
\cdots &= \cdots
\end{aligned}$$

que se reducen de manera que $A > B_1 > B_2 > \cdots$, y que nos lleva, en un número necesariamente finito de pasos, a una ecuación reducida del tipo

$$x^2 - y^2 = Dz^2. \tag{1.11}$$

Y aunque podríamos haber seguido hasta el final, hasta llegar a la ecuación $x^2-y^2 = z^2$, de la que ya obviamente conocemos una solución suya $(1, 0, 1)$, no obstante la anterior $x^2 - y^2 = Dz^2$ ya era fácilmente resoluble:

Descompongamos D en dos factores $\alpha\beta = D$, que no podrán tener cuadrados por no tenerlos D y supongamos $z = 2XY$ con X, Y parámetros enteros arbitrarios. Entonces,

$$(x + y)(x - y) = 4\alpha\beta X^2Y^2$$

tomando $x + y = 2\alpha X^2$, $x - y = 2\beta Y^2$, despejando x, y obtenemos una parametrización de infinitas soluciones,

$$\begin{aligned}
x &= \alpha X^2 + \beta Y^2 \\
y &= \alpha X^2 - \beta Y^2 \\
z &= 2XY.
\end{aligned} \tag{1.12}$$

Por tanto la solución general de la ecuación $x^2 - By^2 = Az^2$, se obtiene a partir de las soluciones de $x^2 - y^2 = Dz^2$ y de todas las transformadas que le preceden. Este procedimiento no es rápido ni da unas fórmulas explícitas para encontrar una primera solución.

Esta condición necesaria, para que el procedimiento del descenso pueda iniciarse, que se cumpla que exista un entero α tal que

$$\frac{\alpha^2 - B}{A} \tag{1.13}$$

sea entero, lo es a cada una de las demás ecuaciones de la sucesión para que el descenso no se interrumpa. Por lo tanto, si la ecuación de partida no la satisface, la ecuación no es resoluble, pero tampoco lo será si en algún momento se interrumpe el descenso porque una de las ecuaciones que la siguen no la cumple. Hasta entonces no se sabía procedimiento para conocer a priori si el proceso se interrumpiría.

Legendre en [2] estudia esta ecuación y consigue establecer un criterio que permite conocer a priori su resolubilidad o no. Afirma que es necesario anadir una condición más que debe cumplir la primera ecuación y tan solo otra más su primera transformada $X^2 - BY^2 = A'X^2$ en (1.8), probando primero que,

Lema 1.3 *La ecuación $x^2 - By^2 = Az^2$ con A, B libre de cuadrados, es resoluble si y sólo si existen los enteros α, β, γ tales que*

$$\frac{\alpha^2 - B}{A}, \quad \frac{\beta^2 - A}{B} \quad y \quad \frac{\gamma^2 - A'}{B} \tag{1.14}$$

sean enteros.

y seguidamente observa y prueba que esta tercera condición es supérflua si A, B son primos entre si,

Teorema 1.1 (Suficiencia en $x^2 - By^2 = Az^2$, Legendre) *La ecuación*

$$x^2 - By^2 = Az^2$$

con,

1. *A, B libres de cuadrados,*
2. *A, B primos dos a dos,*

es resoluble si,

(i) *A es residuo cuadrático a B, y B es residuo cuadrático de A.*

Como la dificultad parece venir del hecho de que los coeficientes de la ecuación $x^2 - By^2 = Az^2$ no son primos dos a dos, Legendre considera entonces una ecuación parecida en la que además de ser libre de cuadrados, sus coeficientes son primos dos a dos. Para ello basta considerar, si $a{=}(A, B)$ es el máximo común divisor de A y B,

$$b = \frac{-B}{a}, \quad c = \frac{-A}{a},$$

para obtener una nueva ecuación,

$$ax^2 + by^2 + cz^2 = 0, \tag{1.15}$$

que es resoluble si y sólo lo es $x^2 - By^2 = Az^2$, porque sus indeterminadas también están relacionadas linealmente:

Si (x_o, y_o, z_o) es solución de $x^2 - By^2 = Az^2$, entonces lo es (x_o, ay_o, az_o) de $ax^2 + by^2 + cz^2 = 0$.

Si (x_o, y_o, z_o) es solución de $ax^2+by^2+cz^2 = 0$, entonces lo es (ax_o, y_o, z_o) de $x^2 - By^2 = Az^2$.

Esta ecuación es sobre la cual Legendre enuncia y prueba su famoso teorema:

Teorema 1.2 (Teorema de Legendre) *La ecuación*

$$ax^2 + by^2 + cz^2 = 0,$$

con a, b, c libre de cuadrados y primos dos a dos, tiene solución no trivial si y sólo si, no todas a, b, c tienen el mismo signo y si existen tres enteros λ, μ, ν tales que

$$\frac{a\lambda^2 + b}{c}, \quad \frac{c\mu^2 + b}{a}, \quad \frac{c\nu^2 + a}{b} \tag{1.16}$$

sean enteros.

Gauss en [3] reformula el enunciado del teorema a otro equivalente, utilizando ya el concepto de resíduo cuadrático como se conoce ahora, a la vez que da otra demostración a partir de su teoría de formas cuadráticas ternarias en $\mathbb{Z}$.

Teorema 1.3 (de Legendre enunciado de Gauss) *La ecuación*

$$ax^2 + by^2 + cz^2 = 0,$$

con a, b, c libre de cuadrados y primos dos a dos, tiene solución no trivial si y sólo si, no todas a, b, c tienen el mismo signo y si $-bc$, $-ca$ y $-ab$ son residuos cuadráticos de a, b y c respectivamente.

Solucionado el problema de la resolubilidad queda pendiente el de hallar alguna solución que no pase por el procedimiento anteriormente descrito. No existen fórmulas conocidas que en términos de los coeficientes a, b, c pueda dar el valor de una solución. La imposibilidad de que existan parece que es consecuencia del décimo problema de Hilbert, pero tampoco se ha probado que no sea posible para este caso particular de ecuación diofántica.

Lo que si es posible es, a partir de una solución conocida, hallar todas las demás paramétricamente que son infinitas. Lo vemos en detalle en el capítulo 3.

En 1950 Holzer [12] prueba que las ecuaciones resolubles tienen al menos una solución (x, y, z) que satisface las cotas,

$$|x| \leq \sqrt{|bc|}, \quad |y| \leq \sqrt{|ac|}, \quad |z| \leq \sqrt{|ab|}, \tag{1.17}$$

con lo que en el peor de los casos, si los coeficientes no son muy grandes, pueden ser halladas por tanteo.

Esencialmente esto es todo lo que se conoce en los enteros acerca de esta ecuación,

$$ax^2 + by^2 + cz^2 = 0,$$

que se conoce como la **Ecuación de Legendre**.

Los resultados acerca de las ecuaciones diofánticas lineales y de los sistemas lineales son de fácil generalización, cuando la ecuación y sus posibles soluciones, son consideradas en otro dominio euclídeo distinto del de los enteros.

Un dominio euclídeo es un dominio que satisface,

Definición 1.2 *Un dominio de integridad A es un* **dominio euclídeo**, *si existe una aplicación N entre los elementos no nulos de A y los naturales satisfaciendo que*

1. *Si $a, b \in A - \{0\}$ y a divide a b entonces $N(a) \leq N(b)$,*

2. **División entera**. *Dados* $a, b \in A$, $b \neq 0$, *existen* q *y* r *tales que* $a = qb + r$ *y con* $N(r) < N(b)$ *si* $r \neq 0$.

A esta aplicación N se le suele llamar **norma euclídea**, y no debemos confundirla con la norma en el sentido clásico vectorial ya que la norma euclídea no necesariamente cumple la desigualdad triangular.

En la ecuación cuadrática, porque no se han encontrado contraejemplo, parece que también los resultados son generalizables automáticamente.

No obstante, la clave de los argumentos para probar que la condición,

$-bc$, $-ca$ y $-ab$ son residuos cuadráticos de a, b y c respectivamente,

es suficiente [4] en otro dominio euclídeo distinto a $\mathbb{Z}$ para la prueba del teorema de Legendre, requiere que fuera cierta la desigualdad triangular para la norma euclídea definida si queremos generalizar el razonamiento dado en la ecuación (1.9). Y eso no es siempre cierto. Por ejemplo, sí satisface la desigualdad triangular con la norma:= valor absoluto en $\mathbb{Z}$, no lo hace con la norma $N(a + bi) := a^2 + b^2$ definida en los enteros de Gauss $\mathbb{Z}[i]$ y tampoco con la norma $|p|$:= grado del polinomio p, en el anillo de los polinomios racionales $\mathbb{Q}[t]$.

Pero no sólo eso, existe la dificultad que plantean las ecuaciones con las unidades. En $\mathbb{Z}$ se reduce sólo a la ecuación $x^2 + y^2 = z^2$ que sabemos resoluble, en $\mathbb{Z}[i]$ como veremos en la sección 5.4 se reducen a

$$x^2 + y^2 + \epsilon z^2 = 0 \qquad x^2 - y^2 = \epsilon z^2$$

con ϵ unidad $\in \{1, -1, i, -i\}$ pero en $\mathbb{Q}[t]$ hay infinitas, tantas como ecuaciones enteras resolubles.

Samet [15] logra demostrar el teorema similar para la ecuación de legendre $ax^2 + by^2 + cz^2 = 0$ en $\mathbb{Z}[i]$ expresada en su forma normal, que tiene solución si y sólo si bc, ca, ab son residuos cuadráticos de a, b y c respectivamente, omitiendo en las condiciones el signo negativo ya que $i^2 = -1$. [5] En el capítulo 5 hacemos una demostración en detalle, mostrando la manera en la que esta generalización es posible en $\mathbb{Z}[i]$.

[4] A esta condición hay que añadirle alguna condición dependiendo del dominio euclídeo. Por ejemplo en $\mathbb{Z}$ es que no todos los a, b c tienen el mismo signo, en $\mathbb{Z}[i]$, anillo de los enteros de Gauss, no es necesario condición adicional y en $\mathbb{Q}[t]$ anillo de los polinomios racionales, lo es que la ecuación con los coeficientes de mayor grado de a, b, c es resoluble en $\mathbb{Z}$, como probaré en el capítulo 7.

[5] Ver las propiedades de los resíduos en el teorema 2.4

Hemer [16] lo prueba en otros dominios euclídeos imaginarios.

El propio Samet comenta en su artículo, que no ha sido capaz de probar el teorema de Holzer en $\mathbb{Z}[i]$, y hasta el momento presente, no se habían probado resultados sobre las cotas de las soluciones para la ecuación de Legendre en $\mathbb{Z}[i]$.

El caso es que el teorema de Holzer no se cumple en los enteros de Gauss, al menos como en su redacción original en los enteros. Por ejemplo, la ecuación

$$ix^2 + 7y^2 + z^2 = 0$$

tiene como solución más pequeña a $(2+2i, 1, 1)$, en donde $|x| = |2+2i| = \sqrt{8} > \sqrt{|bc|} = \sqrt{|7|}$. Aquí, el valor absoluto es generalizado por el módulo del complejo.

Pero es posible adaptar las cotas de Holzer ateniéndonos a las características del dominio euclídeo $\mathbb{Z}[i]$. En el capítulo 6 de esta tesis, publicado en [29], se prueba que al menos se cumple el siguiente teorema:

Teorema 1.4 *La ecuación $ax^2 + by^2 + cz^2 = 0$ en $\mathbb{Z}[i]$ expresada en su forma normal, si tiene soluciones, entonces tiene una (x, y, z) con,*

$$|z| \leq \sqrt{(1+\sqrt{2})|ab|}.$$

He intentado sin conseguir probar, que esta desigualdad se da en las tres variables simultáneamente para alguna solución, como en los enteros,

$$|x| \leq \sqrt{(1+\sqrt{2})|bc|}, \quad |y| \leq \sqrt{(1+\sqrt{2})|ac|}, \quad |z| \leq \sqrt{(1+\sqrt{2})|ab|}.$$

Tampoco he encontrado ejemplo de que no sea cierto.

Tambien se prueba en esta tesis la generalización del teorema de Legendre en el dominio euclídeo de los polinomios con coeficientes racionales $\mathbb{Q}[t]$.

En el anillo de los polinomios racionales es diferente. Puesto que su sistema de clases residuales módulo un polinomio q de grado cero se reduce a un único elemento,

$$\mathbb{Q}[t]_q = \{[0]_q\},$$

porque el resto en la división de un racional por un racional es siempre 0, cualquier racional es entonces siempre residuo cuadrático módulo cualquier polinomio de grado cero. Esto hace que obviamente el teorema de Legendre no se cumpla para los polinomios de grado 0 si no es enunciado de

alguna manera que permita incluir a las ecuaciones con polinomios de grado 0 aparte.

El teorema que se prueba en esta tesis, en el capítulo 7, aceptado para su publicación en revisión [30] es,

Teorema 1.5 *La ecuación*

$$ax^2 + by^2 + cz^2 = 0 \tag{1.18}$$

en el anillo de los polinomios $\mathbb{Q}[t]$, con a, b, c con coeficientes enteros, $abc \neq 0$, expresada en su forma normal en $\mathbb{Q}[t]$, es decir

(ii) *a, b, c libre de cuadrados,*

(iii) *a, b, c primos dos a dos en $\mathbb{Z}[t]$*

tiene solución no trivial de valores primos relativos dos a dos en $\mathbb{Q}[t]$ si y sólo si

(i) *$a^o x^2 + b^o y^2 + c^o z^2 = 0$ con a^o, b^o y c^o coeficientes de mayor grado de a, b y c respectivamente es resoluble en $\mathbb{Z}$,*

(iv) *$-bc$, $-ac$, $-ab$ son resíduos cuadrádricos de a, b y c respectivamente en $\mathbb{Q}[t]$.*

Adaptando las cotas de Holzer a las características de $\mathbb{Q}[t]$, se prueba la versión del teorema de Holzer en ese anillo en el capítulo 8, y enviado para su posible publicación [31]

Teorema 1.6 *La ecuación*

$$ax^2 + by^2 + cz^2 = 0 \tag{1.19}$$

con coeficientes a, b, c en los polinomios racionales $\mathbb{Q}[t]$, expresada en su forma normal en $\mathbb{Q}[t]$, si tiene una solución en $\mathbb{Q}[t]$, entonces tiene una solución (x, y, z) en donde

$$|x| \leq \frac{1}{2}(|b| + |c|), \quad |y| \leq \frac{1}{2}(|a| + |c|), \quad |z| \leq \frac{1}{2}(|a| + |b|) \tag{1.20}$$

Donde $|p| :=$ el grado del polinomio p. Si la ecuación está expresada en su forma normal reordenada, es decir con $|a| \leq |b| \leq |c|$, si $|ab|$ es impar entonces las tres desigualdades son estrictas.

Este teorema no nos da información acerca de la magnitud de los coeficientes de las soluciones en $\mathbb{Z}[t]$.

Continuando con la investigación me cuestioné si era posible determinar cuando una ecuación en los polinomios tiene solución entera, probando en el capítulo 9, el teorema que sigue,

Teorema 1.7 *La ecuación*

$$ax^2 + by^2 + cz^2 = 0 \tag{1.21}$$

en $\mathbb{Q}[t]$, expresada en su forma normal, reordenada de manera que los grados de los coeficientes son $|a| \leq |b| \leq |c|$, tiene solución entera (x_o, y_o, z_o) única salvo múltiplos, si y solo si $(y_o/x_o)^2$ y $(z_o/x_o)^2$ son representantes racionales de las clases,

$$[-a/b]_c = [(y_o/x_o)^2]_c, \qquad [-a/c]_b = [(z_o/x_o)^2]_b. \tag{1.22}$$

Este teorema resuelve el problema equivalente de encontrar las soluciones enteras de un sistema de ecuaciones de Legendre:

Teorema 1.8 *El sistema de ecuaciones en $\mathbb{Z}$,*

$$\begin{aligned} a_o x^2 + b_o y^2 + c_o z^2 &= 0 \\ a_1 x^2 + b_1 y^2 + c_1 z^2 &= 0 \\ &\cdots \\ a_n x^2 + b_n y^2 + c_n z^2 &= 0 \end{aligned}$$

con $a = a_o + a_1 t \cdots + a_n t^n$, $b = b_o + b_1 t \cdots + b_n t^n$, $c = c_o + c_1 t \cdots + c_n t^n$ primos dos a dos y libres de cuadrados en $\mathbb{Z}[t]$, tiene una única solución entera (x_o, y_o, z_o), salvo múltiplos, si y sólo si

$$\left[-\frac{(a_o + a_1 t + \cdots + a_n t^n)}{(b_o + b_1 t + \cdots + b_n t^n)}\right]_{c_o + c_1 t + \cdots + c_n t^n} = [(y_o/x_o^2]_{c_o + c_1 t + \cdots + c_n t^n} \tag{1.23}$$

$$\left[-\frac{(a_o + a_1 t + \cdots + a_n t^n)}{(c_o + c_1 t + \cdots + c_n t^n)}\right]_{b_o + b_1 t + \cdots + b_n t^n} = [(z_o/x_o)^2]_{b_o + b_1 t + \cdots + b_n t^n} \tag{1.24}$$

En particular, pruebo que las ecuaciones resolubles de grado hasta 1 en sus coeficientes, siempre tiene solución entera, y hallo una fórmula explícita para su solución:

Teorema 1.9 *La ecuación*

$$(a_o + a_1 t)x^2 + (b_o + b_1 t)y^2 + (c_o + c_1 t)z^2 = 0$$

expresada en su forma normal, con $c_1 \neq 0$*, tiene solución si y sólo si*

$$\frac{a_1 c_o - a_o c_1}{c_1 b_o - c_o b_1}, \quad \frac{b_1 a_o - b_o a_1}{c_1 b_o - c_o b_1},$$

son cuadrados en $\mathbb{Q}$*. En ese caso una solución en* $\mathbb{Q}$ *es*

$$x = 1, \quad y = \sqrt{\frac{a_1 c_o - a_o c_1}{c_1 b_o - c_o b_1}}, \quad z = \sqrt{\frac{b_1 a_o - b_o a_1}{c_1 b_o - c_o b_1}}$$

y la obtenida en $\mathbb{Z}$ *tras eliminar denominadores es la única salvo múltiplos.*

Las posibilidades de generalizaciones de los resultados en otros dominios euclídeos deja abierta una vía para posibles investigaciones y trabajos futuros. En el capítulo 10 enumero algunas ideas.

2

La ecuación de Legendre

La prueba del teorema de Legendre con sus argumentos no quedó definitivamente clara hasta que Dirichlet [6] hiciera una elegante demostración por inducción sobre el índice de la ecuación. Esta demostración clave es la que permite abordar la generalización del teorema en los distintos dominios euclídeos. Pero antes sintetizamos algunas cosas que es necesario tener presente. Empezamos con la ecuación lineal.

2.1 La ecuación lineal

Es conocido que la ecuación,

$$a_1x_1 + a_2x_2 \cdots + a_nx_n = b \tag{2.1}$$

tiene solución en los enteros si y sólo si el máximo común divisor d de los coeficientes divide a b.

Encontrar una solución de la ecuación diofántica más elemental en la teoría de números,

$$a_1x_1 + a_2x_2 = 1, \tag{2.2}$$

puede hacerse con cualquier programa de cálculo simbólico que incorpore una función que la resuelva. Su cálculo se basa en la aplicación reiterada de la división euclídea entre los coeficientes y los sucesivos restos, no obstante los programas de cálculo simbólico hacen la división en los enteros y no nos servirá cuando trabajemos por ejemplo en los enteros de Gauss u otro dominio euclídeo. Detallamos a continuación un procedimiento general para resolverla.

Las división reiterada puede ser interpretada matricialmente en sucesi-

vas transformaciones lineales en las variables. Una parametrización de la soluciones vendrá dada a partir del producto de las matrices de esas transformaciones como sigue:

Podemos suponer que $|a_2| < |a_1|$. Buscamos q_1, r_1, cociente y resto de la división de a_1 por a_2,

$$|a_2 q_1 + a_1| = |r_1| < |a_2|.$$

Consideramos la transformación,

$$\begin{array}{ll} x_1 = \quad x_{11} & \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ q_1 & 1 \end{bmatrix} \begin{bmatrix} x_{11} \\ x_{21} \end{bmatrix} \\ x_2 = q_1 x_{11} + x_{21} & a_1 x_{11} + a_2(q_1 x_{11} + x_{21}) = r_1 x_{11} + a_2 x_{21} = 1. \end{array}$$

La nueva ecuación transformada $r_1 x_{11} + a_2 x_{21} = 1$ tiene ahora el primer coeficiente más pequeño que el segundo $|r_1| < |a_2|$, dividimos a_2 entre r_1, $|r_1 q_2 + a_2| = |r_2| < |r_1|$ y consideramos de nuevo la transformación,

$$\begin{array}{ll} x_{11} = x_{12} + q_2 x_{22} & \begin{bmatrix} x_{11} \\ x_{21} \end{bmatrix} = \begin{bmatrix} 1 & q_2 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} x_{12} \\ x_{22} \end{bmatrix} \\ x_{21} = \qquad x_{22} & r_1(x_{12} + q_2 x_{22}) + a_2 x_{22} = r_1 x_{12} + r_2 x_{22} = 1. \end{array}$$

Como $r_1 > r_2 > \cdots$, repetimos el proceso las veces necesarias hasta que obtengamos, digamos en la k-ésima transformación $r_k = 1$ y la última transformación nos dará que una de las variables es $x_{1k} = 1$ o $x_{2k} = 1$. En cualquier caso tendríamos la parametrización de las soluciones en función de los sucesivos cocientes $q_1, q_2, \cdots, q_k$ y con un sólo parámetro, pongamos X, y como un producto de matrices.

Podemos enunciar entonces,

Proposición 2.1 *Si $q_1, q_2 \cdots q_k$ representan los sucesivos cocientes antes descritos, entonces la ecuación $a_1 x_1 + a_2 x_2 = 1$ tiene solución,*

$$\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ q_1 & 1 \end{bmatrix} \begin{bmatrix} 1 & q_2 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ q_3 & 1 \end{bmatrix} \cdots \begin{bmatrix} 1 & 0 \\ q_k & 1 \end{bmatrix} \begin{bmatrix} X \\ 1 \end{bmatrix}, \qquad (2.3)$$

si k es impar, y

$$\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ q_1 & 1 \end{bmatrix} \begin{bmatrix} 1 & q_2 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ q_3 & 1 \end{bmatrix} \cdots \begin{bmatrix} 1 & q_k \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ X \end{bmatrix}, \tag{2.4}$$

si k es par.

Este proceso puede generalizarse [20] para resolver con $n-1$ parámetros las soluciones de la ecuación $a_1x_1 + a_2x_2 \cdots + a_nx_n = b$.

2.2 La ecuación cuadrática ternaria homogénea

La resolución de las ecuaciones cuadráticas homogéneas en una variable es trivial. En dos variables, la ecuación

$$ax^2 + bxy + cy^2 = 0, \tag{2.5}$$

es sencilla de resolver,

Proposición 2.2 *La ecuación $ax^2+bxy+cy^2 = 0$ tiene solución si y sólo si $b^2 - 4ac = k^2$ es un cuadrado (incluido el 0), y su solución es $(k-b, 2a)$.*

Esto es porque la ecuación puede ser expresada en forma diagonal mediante una transformación lineal en las variables x, y. Para ello, procedemos con matrices elementales en las operaciones de fila y columna hasta tener,

$$\begin{aligned} ax^2 + bxy + cy^2 &= [x, y] \begin{bmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \\ &= [X, Y] \begin{bmatrix} 1 & 0 \\ \frac{-b}{2a} & 1 \end{bmatrix} \begin{bmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{bmatrix} \begin{bmatrix} 1 & \frac{-b}{2a} \\ 0 & 1 \end{bmatrix} \begin{bmatrix} X \\ Y \end{bmatrix} = \\ &= [X, Y] \begin{bmatrix} a & 0 \\ 0 & \frac{-b^2+4ac}{4a} \end{bmatrix} \begin{bmatrix} X \\ Y \end{bmatrix}, \end{aligned}$$

y multiplicando por $4a$, llegamos a la ecuación transformada,

$$4a^2X^2 - (b^2 - 4ac)Y^2 = 0 \quad \text{con} \quad x = 2aX - bY \quad y = 2aY, \tag{2.6}$$

que tiene solución $(k, 2a)$ si y sólo si $b^2 - 4ac = k^2$ es un cuadrado. A su vez $ax^2 + bxy + cy^2 = 0$ tiene entonces la solución $x = 2a(k-b),\ y = 4a^2$ que prescindiendo del factor común es $(k-b, 2a)$.

Con tres variables, la resolubilidad de la ecuación general,

$$ax^2 + bxy + cy^2 + dxz + eyz + fz^2 = 0 \tag{2.7}$$

se reduce a saber si su correspondiente ecuación reducida del tipo de Lagrange $x_1^2 + By_1^2 + Az_1^2$, lo es.

Consideremos la ecuación general, también expresada como una forma cuadrática $X^tGX = 0$,

$$[x, y, z] \begin{bmatrix} a & \frac{b}{2} & \frac{d}{2} \\ \frac{b}{2} & c & \frac{e}{2} \\ \frac{d}{2} & \frac{e}{2} & f \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = 0.$$

Podemos observar primero que,

1. Si a, c, f son todas cero la resolución es trivial, ya que $(1, 0, 0)$ es su solución.

2. También si $b^2 - 4ac = k^2$ es un cuadrado, pudiendo ser también $k = 0$, entonces según la anterior proposición $(2c, k - b, 0)$ es solución. Ygual ocurre con $d^2 - 4af$ y con $e^2 - 4cf$, que tendría por soluciones respectivamente a $(2f, 0, k - d)$ y $(0, 2f, k - e)$.

2.2.1 Formas normales de una ecuación cuadrática ternaria

Entonces para lo que nos interesa, podemos considerar que la ecuación (2.7) tiene al menos uno de los coeficientes, a, c, f distinto de cero y que $b^2 - 4ac$, $d^2 - 4af$, $e^2 - 4cf$ no son ninguno ni cero ni cuadrados. Reordenemos si es necesario las variables de manera que a sea siempre distinto de cero y siendo así diremos que es una ecuación cuadrática ternaria no trivial.

Definición 2.1 *La ecuación $ax^2+bxy+cy^2+dxz+eyz+fz^2 = 0$, es una forma cuadrática ternaria no trivial si tiene al menos uno de los coeficientes, a, c, f distinto de cero y $b^2 - 4ac$, $d^2 - 4af$, $e^2 - 4cf$ no son ninguno ni cero ni cuadrados.*

Entonces tenemos,

Teorema 2.3 *La ecuación $ax^2 + bxy + cy^2 + dxz + eyz + fz^2 = 0$, no*

trivial, tiene solución si y sólo si la tiene $x_1^2 + By_1^2 + Az_1^2 = 0$, *con*

$$B = -(b^2 - 4ac)$$
$$A = -(bd - 2ae)^2 + (b^2 - 4ac)(d^2 - 4af).$$

Esta ecuación no trivial, puede ser reducida mediante una transformada a otra del tipo,

$$x_1^2 + By_1^2 + Az_1^2 = 0. \tag{2.8}$$

Para ello consideramos la transformación lineal $X_1 = TX$,

$$\begin{bmatrix} x_1 \\ y_1 \\ z_1 \end{bmatrix} = \begin{bmatrix} 0 & b^2 - 4ac & bd - 2ae \\ 2a & b & d \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix}, \tag{2.9}$$

que es no singular , $|T| = -2a(b^2 - 4ac) \neq 0$, y (2.7) se transforma en,

$$X^t G X = X^t T^t (T^t)^{-1} G T^{-1} T X = X_1^t [(T^t)^{-1} G T^{-1}] X_1 = X_1^t D X_1$$

una forma racional $X_1^t D X_1$ con D diagonal,

$$D = \frac{-1}{4a(b^2 - 4ac)} \begin{bmatrix} 1 & 0 & 0 \\ 0 & -(b^2 - 4ac) & 0 \\ 0 & 0 & -(bd - 2ae)^2 + (b^2 - 4ac)(d^2 - 4af) \end{bmatrix},$$

en donde si quitamos el factor común $\frac{-1}{4a(b^2-4ac)}$ de los coeficientes para que la forma sea entera, tendremos que (2.7) es resoluble en los enteros si y sólo si lo es $x_1^2 + Ay_1^2 = Bz_1^2$ con,

$$B = -(b^2 - 4ac)$$
$$A = -(bd - 2ae)^2 + (b^2 - 4ac)(d^2 - 4af).$$

donde las soluciones están relacionadas mediante (2.9).

El problema se reduce entonces a la resolución de una ecuación que es del tipo,

$$x^2 + By^2 + Az^2 = 0. \tag{2.10}$$

Como los factores que son cuadrados en los coeficientes de la ecuación resultan irrelevantes para la resolubilidad , si A o B contiene cuadrados, eliminemoslos: Si (2.10) es tal que contiene a α^2, β^2,

$$x^2 + B'\beta^2 y^2 + A'\alpha^2 z^2 = 0,$$

entonces con la transformación,

$$x' = x, \quad y' = \beta y, \quad z' = \alpha z, \tag{2.11}$$

tenemos a $x'^2 + B'y'^2 + A'z'^2 = 0$ que no los contiene. Una ecuación de este tipo libre de cuadrados se dice que es una ecuación reducida de Lagrange que está en su forma normal.

Definición 2.2 *La ecuación $x^2 + By^2 + Az^2 = 0$ es una ecuación reducida de Lagrange en su forma normal si A, B no contienen cuadrados.*

Si a es el máximo común divisor de A y B, llamando $b = B/a$, $c = A/a$ entonces

$$ax^2 + by^2 + cz^2 = 0, \tag{2.12}$$

es el resultado de hacerle a $x^2 + By^2 + Az^2 = 0$ la transformación

$$x \to x, \quad y \to ay, \quad z \to az,$$

que además de no tener cuadrados, tiene los coeficientes primos dos a dos. Si x, y, z es solución de (2.10) entonces lo es x, ay, az de (2.12) y si x, y, z es solución de (2.12) entonces lo es ax, y, z de (2.10). Esta última, que tiene los coeficientes libres de cuadrados y primos dos a dos se conoce como ecuación de Legendre en su forma normal.

Definición 2.3 *La ecuación $ax^2 + by^2 + cz^2 = 0$ de Legendre, está en su forma normal si*

1. *a, b, c son libres de cuadrados.*
2. *a, b, c son primos dos a dos.*

No obstante podríamos haber partido de una ecuación cualquiera de legendre con factores cuadrados y factores comunes por pares y reducirla directamente a su forma nornal. Si partimos de la ecuación cualquiera

$$a_1x_1^2 + b_1y_1^2 + c_1z_1^2 = 0 \tag{2.13}$$

en la que primero, a_1, b_1, c_1 fuesen $a_1 = \alpha^2 a$, $b_1 = \beta^2 b$, $c_1 = \gamma^2 c$ con a, b, c libre de cuadrados, entonces la correspondencia entre las soluciones de (2.13) y las de 2.12 son de manera que si (x_1, y_1, z_1) es solución de (2.13) entonces lo es $(\alpha x_1, \beta y_1, \gamma z_1)$ de (2.12), y si (x, y, z) es solución de (2.12)

entonces lo es $(\beta\gamma x, \gamma\alpha y, \alpha\beta z)$ de (2.13). Segundo, si la ecuación (2.12) es tal que p es un divisor primo común de b y c, si (x, y, z) es solución de (2.12) entonces (x, py, pz) lo es de

$$pax_1^2 + \frac{b}{p}y_1^2 + \frac{c}{p}z_1^2 = 0 \tag{2.14}$$

y recíprocamente si (x_1, y_1, z_1) es solución de (2.13), entonces $(x_1, y_1/p, z_1/p)$ lo es de 2.12.

Como $|pa(b/p)(c/p)| = |abc/p| < |abc|$, después de repetir este proceso las veces necesarias llegaremos a una ecuación con los coeficientes primos dos a dos.

2.3 El teorema de Legendre

Antes de detallar la demostración, conviene recordar estas propiedades acerca de los residuos cuadrátricos en general que van a ser usadas en la demostración, y con objeto de facilitar su lectura.

Teorema 2.4 *Sean a, b, c, α, elementos de cualquier anillo eucídeo, se tiene*

(a) *Si $[a]_c = [b]_c$ entonces ab es residuo cuadrático de c.*

(b) *Si a, b son residuos cuadráticos de c, entonces ab es residuo cuadrático de c.*

(c) *Si a es residuo cuadrático de ck, entonces a es residuo cuadrátrico de c.*

(d) *Si ak^2 es residuo cuadrático de c, y (k, c)=1, entonces a es residuo cudrático de c.*

La demostración del lema es inmediata, no depende del dominio euclídeo en donde se trabaje:

(a) Como $[a]_c = [b]_c$, entonces $[a^2]_c = [b^2]_c = [ab]_c$.
(b) Si $[r^2]_c = [a]_c$ y $[s^2]_c = [b]_c$, entonces,

$$[(rs)^2]_c = [ab]_c.$$

(c) Si $[r^2]_{ck} = [a]_{ck}$, entonces $[r^2 - a]_{ck} = [0]_{ck}$, también $[r^2 - a]_c = [0]_c$ y por tanto,

$$[r^2]_c = [a]_c.$$

(d) Si $[r^2]_c = [ak^2]_c$ entonces $[k]_c$ es inversible en $\mathbb{Z}_c$ y se tiene que,

$$[(r/k)^2]_c = [a]_c.$$

2.3.1 Demostración del teorema

El teorema de Legendre enunciado como ahora se conoce es el siguiente:

Teorema 2.5 (de Legendre) *La ecuación en $\mathbb{Z}$,*

$$ax^2 + by^2 + cz^2 = 0, \tag{2.15}$$

es resoluble en $\mathbb{Z}$ si y sólo si,

(i) *no todas a, b, c tienen el mismo signo,*

(iii) *$-bc$, $-ca$ y $-ab$ son residuos cuadráticos de a, b y c respectivamente.*

Es obvio que (i) es necesario para que tenga solución, probamos que lo es (iii) con el lema que sigue, similar al lema (1.2) .

Lema 2.1 (Lagrange. Necesidad de (iii)) *Si la ecuación $ax^2+by^2+cz^2 = 0$, expresada en su forma normal, tiene solución en $\mathbb{Z}$ entonces es necesario que,*

(iii) $-bc, -ac, -ab$ sean residuos cuadráticos de $a, b,$ y c respectivamente.

La demostración de la necesidad de (iii) no depende del dominio euclídeo $\mathbb{E}$ en el que se defina la ecuación. Para su demostración, observamos primero que si x_o, y_o, z_o es solución primitiva, es decir con (x_o, y_o, z_o)=1, entonces

$$(x_o, y_o) = (x_o, z_o) = (y_o, z_o) = 1,^{1}$$

ya que si fuese $(x_o, y_o)\neq 1$ tendríamos $x_o = px'$, $y_o = py'$ con p primo común con $-cz_o^2 = a(px')^2 + b(py')^2$, y entonces $[-cz_o^2]_{p^2} = [p^2]_{p^2}[ax'^2 + by'^2]_{p^2} = [0]_{p^2}$ lo que no es posible ya que p no divide a z_o y p^2 no o hace a z_o^2, y tampoco p^2 divide a c que está libre de cuadrados.

[1] Si estamos en cualquier dominio $\mathbb{E}$, entonces 1 es el representante del grupo de unidades. En $\mathbb{Z}$ es $\{1, -1\}$, en $\mathbb{Z}[i]$ es $\{1, -1, i, -i\}$ y en $\mathbb{Q}[t]$ son todos los racionales exepto el 0.

Segundo, también es cierto que

$$(x_o, c) = 1,$$

ya que si p fuera un primo común debería dividir a by_o^2, no lo hace a b por ser b, c primos entre si, y no lo hace a y_o^2 ni a y_o por ser x_o e y_o como hemos visto, primos entre si. Por tanto x_o es siempre inversible en el anillo de las clases residuales $\mathbb{E}_c$.

Siendo así, como $ax_o^2 + by_o^2 = -cz_o^2$ entonces $[ax_o^2 + by_o^2]_c = [0]_c$, y multiplicando por $[(1/x_o)^2 b]_c$ se tiene $[ab + b^2 y_o^2 (1/x_o)^2]_c = [0]_c$. Por tanto,

$$[(by_o/x_o)^2]_c = [-ab]_c \tag{2.16}$$

y $-ab$ es entonces un residuo cuadrático de c. De forma semejante se prueba que $-bc$, $-ac$ son también residuos cuadráticos de a y b respectivamente. Esto prueba la necesidad de (iii) en $\mathbb{E}$ y en este caso en particular en $\mathbb{Z}$.

Lo más difícil es la suficiencia de (i) y (iii) en $\mathbb{Z}$. Legendre da argumentos para justificar porqué estas condiciones son suficientes. Sus argumentos fueron criticados por Gauss [3] que hace una demostración alternativa como una consecuencia de su teoría de formas ternarias en $\mathbb{Z}$. No obtante esta demostración de Gauss no es generalizable a otros dominios euclídeos, que es lo que nos interesa.

Dirichlet [6], adaptanto los argumentos de Lagrange y Legendre hace una demostración de la suficiencia por inducción sobre el índice (que definimos a continuación) de la ecuación. Esta demostración, también en Dickson [10], si puede adaptarse como veremos más tarde a otros dominios euclídeos. La reproducimos a continuación de la forma más fiel posible a la original.

Teorema 2.6 (Dirichlet. Suficiencia de (i) y (iii)) *Si a, b c son enteros, la ecuación*

$$ax^2 + by^2 + cz^2 = 0$$

tiene soluciones enteras de valores primos dos a dos si

(i) *a, b, c no son todas del mismo signo ni cero,*

(ii) *a,b,c, son primos dos a dos,*

(iii) *-bc, -ac, -ab son residuos cuadráticos de a, b, c, respectivamente,*

(iv) *a,b,c, no tiene factores cuadrados > 1.*

Dirichlet hace la siguiente demostración en 1871, 86 años después que Legendre:

En el caso de que los enteros positivos

$$|bc|, \qquad |ac|, \qquad |ab| \tag{2.17}$$

sean distintos, el **índice** de 2.15 se define como aquel valor de los tres que se encuentra entre los otros dos. Si dos o tres de los números fueran iguales, el índice se define como el valor común de esos dos o tres valores.

Cuando el índice es 1, al menos uno de los números en (2.17) es 1, digamos que $|ab| = 1$. Entonces los números (2.17) son $|c|$, $|c|$, 1, y por tanto $|c| = 1$. También $|a| = |b| = 1$. Pero a, b, c no tienen el mismo signo. Si, por ejemplo, $b = -a$, entonces (2.15) tiene solución $x = 1$, $y = 1$, $z = 0$. El teorema es entonces cierto para las ecuaciones de índice 1.

Para proceder por inducción, asumimos que el teorema es cierto para todas las ecuaciones (2.15) que satisfacen las propiedades (i)-(iv) y teniendo índice menor que J. Supongamos que $J > 1$.

Viendo la simetría de (i)-(iv) en a, b, c, podemos poner

$$|a| \leq |b| \leq |c|. \tag{2.18}$$

Entonces

$$|ab| \leq |ac| \leq |bc|,$$

donde $J = |ac|$.

Como b y c son primos relativos, $|b| = |c|$ implicaría $|b| = |c| = 1$ y $J = 1$, contrario a la hipótesis. Tenemos

$$|a| \leq |b| < |c|, \qquad |ab| < |ac| = J \leq |bc|. \tag{2.19}$$

Por (iii) existen enteros R y r para los cuales

$$[R^2]_c = [-ab]_c, \quad [ar]_c = [R]_c,$$

luego $[ar^2]_c = [-b]_c$. Podemos tomar

$$|r| \leq \frac{1}{2}|c|.$$

Entonces

$$ar^2 + b = cQ, \tag{2.20}$$

$$|Q| \leq \frac{|a|r^2 + |b|}{|c|} \leq \frac{1}{4}|ac| + \left|\frac{b}{c}\right| < \frac{1}{4}J + 1 < J. \tag{2.21}$$

Si Q=0, (2.20) da $|r| = 1$ ya que b no tiene factores cuadrados > 1, y $b = -a$, entonces (2.15) tiene la solución $x = 1$, $y = 1$, $z = 0$.

En adelante podemos suponer que $Q \neq 0$.

Sea A el máximo común divisor (positivo) de los tres términos de (2.20),

$$A = (ar^2, b, cQ).$$

Como cualquier divisor común de ar^2 y de b lo es de la suma $ar^2 + b$, entonces A resulta ser además el máximo común divisor de cualquiera de dos de los tres términos. Ya que A divide el término b, A es primo a a y c. Por tanto A divide r^2 y Q. Pero el divisor A de b no tiene factores cuadrados que sean mayores que 1. Por tanto A divide r.

Puedo entonces escribir

$$r = A\alpha, \qquad b = A\beta, \qquad Q = Aq = AC\gamma^2, \tag{2.22}$$

donde γ^2 es el mayor cuadrado que divide q. Así (2.20) da

$$aA\alpha^2 + \beta = cC\gamma^2, \tag{2.23}$$

cuyos términos son primos dos a dos. Definimos

$$B = a\beta.$$

Probamos que A, B, C tiene las propiedades (I)-(IV) similares a (i)-(iv) con a, b, c sustituídos por A, B, C.

Evidentemente, ninguno de A, B, C son todos del mismo signo.

Como a y b son primos relativos y ninguno tiene factores comunes > 1, $AB = ab$ implica que ninguno de los dos A y B tiene factor > 1, y que A y B son primos relativos.

Como γ^2 es el mayor cuadrado que divide a $q = C\gamma^2$, C no tiene factores cuadrados mayores que 1.

Como los términos de (2.23) son primos dos a dos, C es primo con $aA\beta = AB$. Esto prueba (II) y (IV).

Probamos ahora que A, B, C no tienen todos el mismo signo. Esto es cierto si $ab = AB$ es negativo. Por tanto sea ab positivo. Por (i), ac y bc son entonces negativos. Entonces, por (2.20),

$$c^2 AC\gamma^2 = c^2 Q = acr^2 + bc < 0, \tag{2.24}$$

de donde AC es negativo. Esto completa la prueba de (I).

Por (2.23), cuyos términos son primos dos a dos, vemos que βcC, $acAC$, y $-aA\beta = -AB$ son residuos cuadráticos de aA, β y C respectivamente.

Por (iii), $-bc = -\beta Ac$ es residuo cuadrático de a, y $-ac$ lo es de $b = A\beta$ y por tanto de A.

Como βcC y $-ac$ son residuos cuadrátricos de A, lo mismo es cierto para su producto $-BCc^2$ y por tanto para $-BC$.

Como $-ac$ y $acAC$ son residuos cuadráticos de β, $[u^2]_\beta = [-AC]_\beta$ tiene una solución u.

Como βcC y $-\beta Ac$ y el producto de ambos son residuos cuadráticos de a, $[v^2]_a = [-AC]_a$ tiene una solución v.

Ya que los términos de (2.23) son primos dos a dos, lo mismo es cierto para a y β. Por el teorema chino del resto, existe una solución común w con $[w]_\beta = [u]_\beta$ y con $[w]_a = [v]_a$.

Por tanto $w^2 + AC$ es divisible por β y a y por tanto por $\beta a = B$. Esto completa la demostración de (III).

Por (2.19), (2.21), y (2.22)

$$|AB| = |ab| < J, \qquad |AC| \leq |AC|\gamma^2 = |Q| < J.$$

Por tanto el índice de $AX^2 + BY^2 + CZ^2 = 0$ es $< J$.

Ya que la ecuación tiene las propiedades (I)-(IV), aplico la hipótesis de inducción y tiene una solución entera (X, Y, Z) no trivial.

Pongamos

$$x = A\alpha X - \beta Y, \quad y = X + a\alpha Y, \quad z = C\gamma Z. \tag{2.25}$$

Por (2.22), (2.23), y $B = a\beta$, obtenemos que

$$ax^2 + by^2 + cz^2 = cC\gamma^2(AX^2 + BY^2 + CZ^2) = 0.$$

Si fuese $x = y = 0$ en (2.25), la eliminación de X da $(\beta + Aa\alpha^2)Y = 0$. El primer factor no es cero por (2.20). Entonces $X = 0$, $Y = 0$, y por tanto $Z = 0$ lo que es falso. Luego (2.15) tiene una solución entera no trivial.

Después de esta elegante demostración se han intentado y encontrado demostraciones diferentes, pero son todas ellas específicas para $\mathbb{Z}$ y no generalizables a otros domínios euclídeos.

Por ejemplo la de Gauss [3], la que hacen Davenport y Hall en [11] con métodos de geometría de números, o la de Mordell en [19].

3

Solución general de la ecuación de Legendre

Hasta Lagrange como vimos en la introducción, el procedimiento para encontrar todas las soluciones de una ecuación resoluble del tipo,

$$ax^2 + by^2 + cz^2 = 0$$

expresada en su forma normal sería el siguiente.

Primero transformarla multiplicando por a, y tras eliminar el cuadrado a^2 y hacer $-ab = B$, $-ac = A$ obtener la ecuación de partida $x^2 - By^2 = Az^2$. Formar la sucesión de transformadas que se detallan en la introducción, hasta llegar en un finito de pasos, a una ecuación reducida

$$x^2 - y^2 = Dz^2, \tag{3.1}$$

la cual vimos que si $\alpha\beta = D$ es una descomposición de D, pueden parametrizarse las infinitas soluciones como,

$$\begin{aligned} x &= \alpha X^2 + \beta Y^2 \\ y &= \alpha X^2 - \beta Y^2 \\ z &= 2XY. \end{aligned} \tag{3.2}$$

Lo que no vimos es una justificación acerca de porqué son todas las soluciones.

Llegado a este punto hay que hacer una aclaración.

Si (x_o, y_o, z_o) es solución también lo es $(\pm kx_o, \pm ky_o, \pm kz_o)$, cualquiera que sea el entero k. Pero nos interesa conocer las soluciones (x_o, y_o, z_o)

primitivas, es decir con

$$(x_o, y_o, z_o) = 1,$$

independientemente de los signos, que siempre podemos considerar positivos[1].

Definición 3.1 *Una parametrización es solución general, cuando parametriza todas las soluciones, salvo múltiplos, salvo cambio en los signos.*

Si consideraramos distintas una solución y un múltiplo de ella, es obvio que por ejemplo la terna pitagórica $(5, 4, 3)$, solución de $x^2 - y^2 = z^2$ no es ninguna de las parametrizadas en,

$$\begin{aligned} x &= X^2 + Y^2 \\ y &= X^2 - Y^2 \\ z &= 2XY. \end{aligned}$$

porque z es siempre par.

Pero si consideramos iguales toda las soluciones y múltiplos de ellas con cualquier signo, la parametrización (3.2) si cubre todas las soluciones. Probamos esto último. Consideremos la descomposición de $D = 1 \cdot D$, veamos que la correspondiente parametrización de las soluciones de $x^2 - y^2 = Dz^2$ es solución general.

Teorema 3.1 *Cualquier solución salvo múltiplos de $x^2 - y^2 = Dz^2$, viene expresada mediante*

$$\begin{aligned} x &= X^2 + DY^2 \\ y &= X^2 - DY^2 \\ z &= 2XY. \end{aligned} \tag{3.3}$$

para ciertos valores enteros de X, Y.

Que (x, y, z) es solución, es obvio. Para ver que lo son todas salvo múltiplos, consideremos una solución cualquiera (x_o, y_o, z_o) de (3.1). Si tomamos,[2]

$$X = x_o + y_o, \quad Y = z_o, \tag{3.4}$$

[1] Existen otras investigaciones (ver [28] y su bibliografía) que tratan el problema acerca de cuándo una parametrización cubre todas las soluciones, incluidas las no primitivas, y aquellas con distintos signos

[2] La elección de estos valores para X e Y se justificará en 3.3

entonces sustituimos en (3.3) y obtenemos,

$$\begin{aligned} x = X^2 + DY^2 = (x_o + y_o)^2 + Dy_o^2 = 2x_o y_o + 2x_o \quad &= 2(x_o + y_o)x_o \\ y = X^2 - DY^2 = (x_o + y_o)^2 - Dy_o^2 = 2x_o y_o + 2y_o \quad &= 2(x_o + y_o)y_o \\ z = 2XY \quad &= 2(x_o + y_o)z_o \end{aligned}$$

con lo que, salvo múltiplos, la solución (x, y, z) coincide con (x_o, y_o, z_o).

Por esta vía la solución general de la ecuación de Legendre $ax^2 + by^2 + cz^2 = 0$ se obtendría a partir de las soluciones de $x^2 - y^2 = Dz^2$ y de todas las que le preceden. Las fórmulas que resultarán serán siempre tres formas cuadráticas binarias en X e Y,

$$x = (X, Y)\, Q_x \begin{pmatrix} X \\ Y \end{pmatrix}, \quad y = (X, Y)\, Q_y \begin{pmatrix} X \\ Y \end{pmatrix}, \quad y = (X, Y)\, Q_z \begin{pmatrix} X \\ Y \end{pmatrix}.$$

Este procedimiento para hallar las soluciones, o una fórmula, no es rápido. Sobre todo en los tiempos en los que no existían los ordenadores. Teniendo en cuenta que uno de los problemas siempre a resolver es conocer cuál es la solución más pequeña, aunque partamos de una solución de $x^2 - y^2 = Dz^2$ en magnitud pequeña, nada tenemos asegurado acerca de la magnitud de la solución obtenida finalmente para $ax^2 + by^2 + cz^2 = 0$.

3.1 Solución de Réalis

La primera parametrización directa a partir de la ecuación $ax^2 + by^2 + cz^2 = 0$ la hace Réalis en [7]. Presenta unas fórmulas dependientes de tres parámetros X, Y, Z obtenidas a partir de una solución conocida (x_o, y_o, z_o). Primero, encuentra una solución a partir de (x_o, y_o, z_o),

$$\begin{aligned} &(-a + b + c)x_o - 2(by_o + cz_o) \\ &(a - b + c)y_o - 2(ax_o + cz_o) \\ &(a + b - c)z_o - 2(ax_o + by_o) \end{aligned}$$

después introduce tres parámetros X, Y, Z y tras comprobar que funciona con ejemplos, enuncia sin probar el teorema,

Teorema 3.2 (Réalis) *Si una solución particular de* $ax^2+by^2+cz^2=0$ *viene dada por* (x_o, y_o, z_o)*, la solución general será dada por las fórmulas*

$$\begin{aligned}(-aX^2+bY^2+cZ^2)x_o - 2X(by_oY+cz_oZ)\\ (aX^2-bY^2+cZ^2)y_o - 2Y(ax_oX+cz_oZ)\\ (aX^2+bY^2+cZ^2)z_o - 2Z(ax_oX+by_oY)\end{aligned}$$

con X*,* Y*,* Z *enteros cualesquiera.*

Desconozco si Réalis obvia la demostración porque la considerara fácil o porque no la encontrara, el caso es que las formulas son ciertas y parametrizan todas las soluciones por lo siguiente.

Expresadas de diferente forma, estas fórmulas son las mismas que estas otras

$$\begin{aligned}x_o(aX^2+bY^2+cZ^2) - 2X(ax_oX+by_oY+cz_oZ)\\ y_o(aX^2+bY^2+cZ^2) - 2Y(ax_oX+by_oY+cz_oZ)\\ z_o(aX^2+bY^2+cZ^2) - 2Z(ax_oX+by_oY+cz_oZ).\end{aligned} \tag{3.5}$$

Réalis pudo haber deducido estas fórmulas parametrizando las soluciones imponiendo que,

$$(x_o+tX, y_o+tY, z_o+tZ) \tag{3.6}$$

fuera una solución en los racionales con X, Y, Z parámetros enteros y t racional, $t\neq 0$. Sustituyendo se obtiene,

$$\begin{aligned}0 = a(x_o+tX)^2+b(y_o+tY)^2+c(z_o+tZ)^2 =\\ ax_o^2+2ax_otX+at^2X^2+by_o^2+2by_otY+bt^2Y^2+cz_o^2+2cz_otZ+ct^2Z^2 =\\ ax_o^2+by_o^2+cz_o^2+(aX^2+bY^2+cZ^2)t^2+2t(ax_oX+by_oY+cz_oZ) =\\ t((aX^2+bY^2+cZ^2)t+2(ax_oX+by_oY+cz_oZ)).\end{aligned}$$

Ya que $t\neq 0$ obtengo,

$$t=\frac{-2(ax_oX+by_oY+cz_oZ)}{aX^2+bY^2+cZ^2}$$

que sustituido en (3.6) nos da soluciones en los racionales de la ecuación $ax^2+by^2+cz^2=0$.

Multiplicando por $aX^2+bY^2+cZ^2$ obtengo las mismas soluciones enteras de Réalis de (3.5).

Si reordenamos la ecuación de manera que podamos considerar siempre que a, b son positivos y c negativo, no podrá darse nunca una solución (x_o, y_o, z_o) con $z_o = 0$.

Siendo así, con sólo dos parámetros X, Y, y prescindiendo de Z, haciendo éste que valga 0 en las fórmulas, las que resultan, representan todas las soluciones:

Teorema 3.3 *Si (x_o, y_o, z_o) es solución de $ax^2+by^2+cz^2 = 0$, con $a, b > 0$, $c < 0$, entonces cualquier solución (x, y, z) salvo multiplos, viene expresada mediante*

$$\begin{aligned} x &= x_o(aX^2 + bY^2) - 2X(ax_oX + by_oY) &&= -ax_oX^2 - 2by_oXY + bx_oY^2 \\ y &= y_o(aX^2 + bY^2) - 2Y(ax_oX + by_oY) &&= ay_oX^2 - 2ax_oXY - by_oY^2 \\ z &= z_o(aX^2 + bY^2) \end{aligned} \tag{3.7}$$

para ciertos valores enteros X, Y.

Puede comprobarse operando, que si (x, y, z) es una solución cualquiera, entonces tomando [3],

$$X = b(yz_o + y_oz) \quad Y = -a(xz_o + x_oz) \tag{3.8}$$

obtenemos la solución,

$$\begin{aligned} &2z_o^2(axx_o + byy_o - czz_o)x \\ &2z_o^2(axx_o + byy_o - czz_o)y \\ &2z_o^2(axx_o + byy_o - czz_o)z \end{aligned}$$

que es un múltiplo de la solución (x, y, z).

Las mismas fórmulas que las del teorema, salvo alguna diferencia en los signos, son las que se obtienen mediante enfoques geométricos como vemos a continuación.

[3] La elección de estos valores para X e Y se justifica en 3.3

3.2 Solución como intersección de recta y elipse

Después de cambiar el signo y reordenar los coeficientes si fuera necesario, expresemos la ecuación de Legendre con $a > 0$, $b > 0$ y $c > 0$ de la forma

$$ax^2 + by^2 = cz^2.$$

Dividiendo por cz^2, la ecuación 2.15 representa una elipse en el plano

$$\frac{a}{c}\left(\frac{x}{z}\right)^2 + \frac{b}{c}\left(\frac{y}{z}\right)^2 = 1.$$

Si disponemos de una solución x_o, y_o, z_o de la ecuación, tenemos un punto de la elipse de coordenadas racionales

$$\left(\frac{x_o}{z_o}, \frac{y_o}{z_o}\right),$$

y cualquier otra solución de la ecuación es otro punto de coordenadas racionales $\left(\frac{x}{z}, \frac{y}{z}\right)$ que está sobre la elipse.

Para hallarlos basta observar que el corte de una recta que pasa por $\left(\frac{x_o}{z_o}, \frac{y_o}{z_o}\right)$ de pendiente $-\frac{Y}{X}$ cualquiera, X, Y enteros, con la elipse, es siempre un punto de coordenadas racionales:

La recta en paramétricas es

$$\frac{x}{z} = \frac{x_o}{z_o} + tX, \qquad \frac{y}{z} = \frac{y_o}{z_o} + tY. \tag{3.9}$$

Imponiendo

$$\frac{a}{c}\left(\frac{x_o}{z_o} + tX\right)^2 + \frac{b}{c}\left(\frac{y_o}{z_o} + tY\right)^2 = 1,$$

y teniendo en cuenta que $ax_o^2 + by_o^2 - cz_o^2 = 0$, despejo t

$$t = -\frac{2(ax_oX + by_oY)}{az_oX^2 + bz_oY^2}$$

que sustituido en 3.9, y una vez eliminados denominadores nos dan las mismas parametrizaciones que las del teorema 3.3

3.3 Solución mediante reflexión de vectores G-unitarios

Consideremos $\mathbb{Q}_G^2$, el espacio euclídeo de los vectores racionales, pero, con el producto escalar definido como:

$$\vec{v} \cdot \vec{w} := \vec{v}\, G\, \vec{w}^t \quad \text{con} \quad G = \begin{pmatrix} a/c & 0 \\ 0 & b/c \end{pmatrix}.$$

En este espacio la norma de un vector de cordenadas racionales $(\frac{x}{z}, \frac{y}{z})$ respecto a cualquier base, es

$$\sqrt{\left(\frac{x}{z}, \frac{y}{z}\right) G \left(\frac{x}{z}, \frac{y}{z}\right)^t} = \sqrt{\frac{a}{c}\left(\frac{x}{z}\right)^2 + \frac{b}{c}\left(\frac{y}{z}\right)^2}$$

y entonces,

Definición 3.2 *$(\frac{x}{z}, \frac{y}{z})$ es G-unitario si y sólo si sus coordenadas son soluciones racionales de la ecuación*

$$\frac{a}{c}\left(\frac{x}{z}\right)^2 + \frac{b}{c}\left(\frac{y}{z}\right)^2 = 1.$$

Todas las soluciones tienen en común ser coordenadas de vectores unitarios de $\mathbb{Q}_G^2$, de manera que ahora encontrar las soluciones de 2.15 se reduce a encontrar los vectores $(\frac{x}{z}, \frac{y}{z})$ unitarios en $\mathbb{Q}_G^2$.

Conocida pues una solución $(x_o, y_o z_o)$, el vector solución

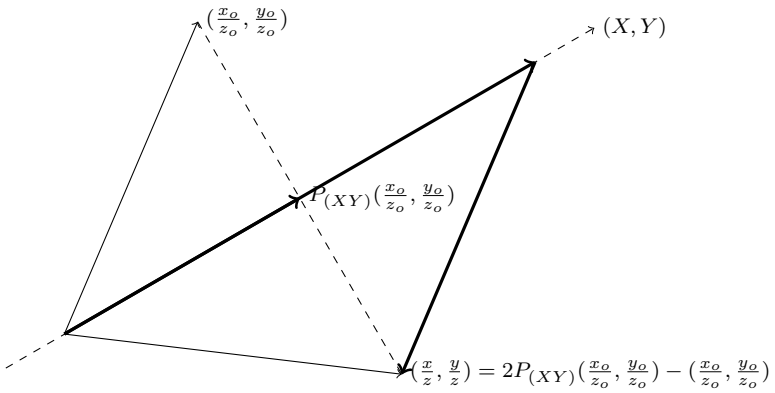
$$\left(\frac{x_o}{z_o}, \frac{y_o}{z_o}\right)$$

es unitario en $\mathbb{Q}_G^2$, y encontrar todos los demás puede hacerse mediante isometrías.

Las isometrías preservan las distancias, y transforman vectores unitarios en vectores unitarios: Hacemos una reflexión del vector solución respecto a la recta de dirección (X, Y).

El vector $\left(\frac{x}{z}, \frac{y}{z}\right)$ reflejado de $\left(\frac{x_o}{z_o}, \frac{y_o}{z_o}\right)$ respecto a la dirección (X, Y) es dos veces la proyección del vector sobre esa dirección menos el vector:

$$\left(\frac{x}{z}, \frac{y}{z}\right) = 2P_{(X,Y)}\left(\frac{x_o}{z_o}, \frac{y_o}{z_o}\right) - \left(\frac{x_o}{z_o}, \frac{y_o}{z_o}\right) \tag{3.10}$$



De la ecuación,

$$\left(\frac{x}{z}, \frac{y}{z}\right) = 2\frac{\left(\frac{x_o}{z_o}, \frac{y_o}{z_o}\right) G\,(X,Y)^t}{(X,Y)\,G\,(X,Y)^t}(X,Y) - \left(\frac{x_o}{z_o}, \frac{y_o}{z_o}\right)$$

operando y simplificando queda:

$$\left(\frac{ax_oX^2 + 2by_oXY - bx_oY^2}{z_o(aX^2+bY^2)}, \frac{-ay_oX^2 + 2ax_oXY + by_oY^2}{z_o(aX^2+bY^2)}\right) \tag{3.11}$$

de la que eliminando denominador nos da la misma solución entera que en (3.7), aunque con un irrelevantemente cambio de signo en x e y. Podemos enunciar,

Teorema 3.4 *Sea (x_o, y_o, z_o) una solución no trivial de $ax^2+by^2+cz^2 = 0$, con $a, b > 0$, $c < 0$. Sea $G = \begin{pmatrix} a/c & 0 \\ 0 & b/c \end{pmatrix}$. Entonces cualquier otra solución (x, y, z) es tal que,*

$$\left(\frac{x}{z}, \frac{y}{z}\right) = 2\frac{\left(\frac{x_o}{z_o}, \frac{y_o}{z_o}\right) G\,(X,Y)^t}{(X,Y)\,G\,(X,Y)^t}(X,Y) - \left(\frac{x_o}{z_o}, \frac{y_o}{z_o}\right).$$

Queda por ver que todas las soluciones son éstas. Es fácil de verlo geométricamente si observamos que la suma de $\left(\frac{x_o}{z_o}, \frac{y_o}{z_o}\right)$ y de su vector reflejado $\left(\frac{x}{z}, \frac{y}{z}\right)$,

$$\left(\frac{x_o}{z_o} + \frac{x}{z}, \frac{y_o}{z_o} + \frac{y}{z}\right) \tag{3.12}$$

es la dirección (X, Y) de la reflexión, por lo que que una vez sumados y eliminados los denominadores para obtener valores enteros, nos queda que los parámetros que determian la dirección (X, Y) a través de la cual el vector unitario $\left(\frac{x_o}{z_o}, \frac{y_o}{z_o}\right)$ se refleja en $\left(\frac{x}{z}, \frac{y}{z}\right)$ y recíprocamente es

$$X = x_o z + x z_o, \qquad Y = y_o z + y z_o. \tag{3.13}$$

Esto prueba que son todas.

Esto último fundamentó la elección de (3.4). En cuanto la elección de los valores de los parámetros en (3.8), tenemos que la parametrización de (3.7) representa el vector $-\left(\frac{x}{z}, \frac{y}{z}\right)$ de (3.11). Mediante la observación geométrica de que la reflexión de un vector respecto a una dirección y la reflexión del mismo vector respecto a la dirección perpendicular, son los mismos de signo opuesto, sólo tenemos que tomar el perpendicular. Con este producto escalar el vector perpendicular a (X, Y) es,

$$(bY, -aX), \tag{3.14}$$

porque $(X, Y)\, G\, (bY, -ax)^t = 0$. Como tenemos,

$$-R_{(X,Y)}\left(\frac{x_o}{z_o}, \frac{y_o}{z_o}\right) = R_{(bY,-aX)}\left(\frac{x_o}{z_o}, \frac{y_o}{z_o}\right), \tag{3.15}$$

la elección de (3.8) fue el vector perpendicular a (3.13),

$$X = b(y z_o + y_o z) \quad Y = -a(x z_o + x_o z). \tag{3.16}$$

La diferencia en el uso de dos o tres parámetros es la siguiente. La parametrización con dos parámetros X e Y del teorema 3.3

$$\begin{aligned} &x_o(aX^2 + bY^2) - 2X(a x_o X + b y_o Y) \\ &y_o(aX^2 + bY^2) - 2Y(a x_o X + b y_o Y) \\ &z_o(aX^2 + bY^2) \end{aligned} \tag{3.17}$$

dan soluciones que son independientes de los parámetros. Es decir, si hacemos una eliminación de X e Y en las formulas despejando X en una, sustituyendo en las otras dos y volviendo a despejar Y y sustituir en la restante, sólo obtenemos una intratable relación entre las soluciones (x, y, z)

y (x_o, y_o, z_o) [4]. En realidad pueden sustituirse X, Y por cualquier forma lineal en X e Y.

En cambio en la parametrización de Réalis que usa Mordell con un parámero Z más,

$$\begin{aligned} x_o(aX^2+bY^2+cZ^2) - 2X(ax_oX+by_oY+cz_oZ) \\ y_o(aX^2+bY^2+cZ^2) - 2Y(ax_oX+by_oY+cz_oZ) \\ z_o(aX^2+bY^2+cZ^2) - 2Z(ax_oX+by_oY+cz_oZ) \end{aligned} \tag{3.18}$$

las soluciones si dependen de los parámetros. Esto nos permite seleccionar X, Y, Z con algún criterio para buscar una solución que nos convenga, como haremos en la demostración del teorema de Holzer.

3.4 Ecuaciones que satisfacen una solución

En el transcurso de mi investigación necesité disponer de ejemplos de ecuaciones de Legendre resolubles. Ejemplos en distintos dominios euclídeos y con caracteristicas diferentes. La forma más rápida es la de construir una ecuación a partir de una solución que debe satisfacer.

El teorema que sigue resuelve el problema recíproco de encontrar ecuaciones que satisfacen cierta solución dada.

Teorema 3.5 *Sea x_o, y_o, z_o una terna de valores en cualquier dominio euclídeo E, entonces la ecuación general de las ecuaciones de Legendre que satisface $ax_o^2+by_o^2+cz_o^2=0$ vienen dadas por,*

$$\begin{aligned} a = \quad & y_o^2X - z_o^2Y \\ b = -& x_o^2X + z_o^2Z \\ c = \quad & x_o^2Y - y_o^2Z. \end{aligned}$$

con X, Y, Z parámetros en E.

[4] De hecho, según WxMaxima después de eliminar X e Y la relación que resulta es $256a^{10}b^4(b^2y_o^4+2abx_o^2y_o^2+a^2x_o^4)^2(((4b^3x^2y^2+4ab^2x^4)y_o^4+x_o^2(4ab^2x^2y^2+4a^2bx^4)y_o^2+x_o^4(ab^2y^4+2a^2bx^2y^2+a^3x^4))z_o^4+(x_o^2(-4b^3y^3-4ab^2x^2y)y_o^3+x_o^4(-4ab^2y^3-4a^2bx^2y)y_o)zz_o^3+(-4b^3x^2y_o^6-8ab^2x^2x_o^2y_o^4+x_o^4(-2ab^2y^2-6a^2bx^2)y_o^2+x_o^6(-2a^2by^2-2a^3x^2))z^2z_o^2+(4b^3x_o^2yy_o^5+8ab^2x_o^4yy_o^3+4a^2bx_o^6yy_o)z^3z_o+(ab^2x_o^4y_o^4+2a^2bx_o^6y_o^2+a^3x_o^8)z^4)^2=0.$

Como,

$$\begin{aligned} &ax_o^2 + by_o^2 + cz_o^2 = \\ &= (y_o^2X - z_o^2Y)x_o^2 + (-x_o^2X + z_o^2Z)y_o^2 + (x_o^2Y - y_o^2Z)z_o^2 = 0, \end{aligned}$$

es evidente que $ax^2 + by^2 + cz^2 = 0$ es ecuación que satisface x_o, y_o, z_o. Veamos que son todas.

Supongamos que $ax^2+by^2+cz^2 = 0$ es ecuación de Legendre con solución x_o, y_o, z_o veamos que X, Y, X pueden ser elegidos para obtener a, b, c.

Al ser $(x_o, y_o) = 1$ sean N, M tales que,

$$c = x_o^2N - y_o^2M, \tag{3.19}$$

entonces $ax_o^2 + by_o^2 = -cz_o^2 = (y_o^2M - x_o^2N)z_o^2$ y obtenemos,

$$x_o^2(a + z_o^2N) + y_o^2(z_o^2M - b) = 0.$$

También, cualquiera que sea r en E se tiene

$$x_o^2(a + z_o^2N - y_o^2r) + y_o^2(z_o^2M - b + x_o^2r) = 0, \tag{3.20}$$

que al ser $(x_o, y_o) = 1$ sólo es posible si,

$$y_o^2 = a + z_o^2N - y_o^2r, \quad x_o^2 = -(b - z_o^2M + x_o^2r).$$

Llamamos $R = r + 1$, despejamos a, b y tenemos,

$$\begin{aligned} a = &\quad y_o^2R - z_o^2N \\ b = &-x_o^2R + x_o^2M. \end{aligned}$$

Sean X, T tales que

$$R = X - z_o^2T,$$

y las ecuaciones anteriores junto con (3.19) se transforman en,

$$\begin{array}{lcll} a = y_o^2(X - z_o^2T) - z_o^2N & = & y_o^2X & -z_o^2(N + y_o^2T) \\ b = -x_o^2(X - z_o^2T) + z_o^2M & = & -x_o^2X & +z_o^2(N + y_o^2T) \\ c = x_o^2N - y_o^2M & = & x_o^2(N + y_o^2T) & -y_o^2(M + x_o^2T) \end{array}$$

por tanto tomando X, Y, Z con los valores,

$$\begin{aligned} X &= X \\ Y &= N + y_o^2 T \\ Z &= M + x_o^2 T \end{aligned}$$

obtendremos los valores de a, b, c.

El siguiente teorema nos asegura la existencia de una ecuación de legendre con los coeficientes no demasiado grandes respecto a la solución, estando los coeficientes acotados por el módulo

$$||(x_o, y_o, z_o)|| = \sqrt{x_o^2 + y_o^2 + z_o^2}$$

de la solución considerada vectorialmente.

Teorema 3.6 *Dada la terna de enteros x_o, y_o, z_o, existe una ecuación de legendre $ax^2 + by^2 + cz^2 = 0$ con*

$$|a| \leq \sqrt{x_o^2 + y_o^2 + z_o^2}, \quad |b| \leq \sqrt{x_o^2 + y_o^2 + z_o^2}, \quad |c| \leq \sqrt{x_o^2 + y_o^2 + z_o^2} \quad (3.21)$$

Consideremos la función entera

$$f(x, y, z) := x_o^2 x + y_o^2 y + z_o^2 z.$$

Sea N la parte entera de $\sqrt{x_o^2 + y_o^2 + z_o^2}$. Entonces

$$N^2 < x_o 2 + y_o^2 + z_o^2 < (N+1)^2$$

Sea (x, y, z) una terna cualquiera del conjunto $\{0, 1, 2, \cdots, N\}^3$.

En total hay $(N+1)^3$ distintas ternas.

Y el número máximo de posibles valores que puede tomar f es

$$\leq x_o^2 N + y_o^2 N + z_o^2 N = (x_o^2 + y_o^2 + z_o^2)N < (N+1)^2 N$$

pero por el principio del palomar, al haber más ternas que posibles evaluaciones de las mismas, hay dos ternas

$$(x_1, y_1, z_1) \quad (x_2, y_2, z_2)$$

que toman el mismo valor, y cuya diferencia

$$(x_1 - x_2, y_1 - y_2, z_1 - z_2) = (a, b, c)$$

es solución de $f = 0$ que satisface,

$$|a| \leq N, \quad |b| \leq N, \quad |c| \leq N,$$

por encontrarse en ese cubo de arista N, la condición del teorema.

Una parametrización con dos parámetros es también posible. El procedimiento para hallarlas es rápido si $(x_o, y_o) = 1$.

Resolvemos la ecuación lineal,

$$x_o^2 a + y_o^2 b + z_o^2 c = 0, \tag{3.22}$$

sea a_o, b_o solución de $x_o^2 a + y_o^2 b = 1$, entonces para cualquier X

$$x_o^2(z_o^2 c a_o + y_o^2 X) + y_o^2(z_o^2 c b_o - x_o^2 X) + z_o^2 c = 0 \tag{3.23}$$

y la solución general es

$$\begin{aligned} a &= z_o^2 a_o Y + y_o^2 X \\ b &= z_o^2 b_o Y - x_o^2 X \\ c &= Y. \end{aligned}$$

Podemos tomar Y con $|Y| < \frac{x_o^2}{2}$, tomar X con $|b| = |z_o^2 Y b_o - x_o^2 X| < \frac{x_o^2}{2}$ y entonces

$$|a| = |z_o^2 Y a_o + y_o^2 X| \leq \frac{z_o^2}{x_o^2}|Y| + \frac{y_o^2}{x_o^2}|z_o^2 Y b_o - x_o^2 X| < \frac{z_o^2 + y_o^2}{2},$$

y obtendremos una ecuación con

$$|a| < \frac{z_o^2 + y_o^2}{2}, \quad |b| < \frac{x_o^2}{2}, \quad |c| < \frac{x_o^2}{2}.$$

Es posible también obtener una parametrización con dos parámetros aunque x_o, y_o, z_o no sean primos dos a dos. El procedimiento utiliza una generalización del algoritmo de Euclídes para más de dos enteros, similar al expuesto en la proposición 2.1.

4

El teorema de Holzer

Se sabe parametrizar todas las soluciones a partir de una, que puede encontrarse algoritmicamente como vimos con anterioridad por el procedimiento del descenso de Lagrange [1]. Pero esa primera solución obtenida previsiblemente será de gran magnitud. Considerando una solución (x, y, z) como un vector, hay dos normas vectoriales (no normas eucídeas en un dominio) que son comunmente usadas en la investigación de pequeñas soluciones de la ecuación de Legendre.

Previamente observemos que cualesquiera que sean los signos de a, b, y c podemos considerar, después de multiplicar la ecuación por -1 si fuera necesario y reordenados en su caso los coeficientes, la ecuación de Legendre como

$$ax^2 + by^2 = cz^2 \tag{4.1}$$

donde

$$a > 0, \quad b > 0 \quad \text{y} \quad c > 0.$$

La primera norma es la norma ponderada del supremo,

$$||(x, y, z)||_1 = \max \left\{ \frac{x}{\sqrt{bc}}, \frac{y}{\sqrt{ac}}, \frac{z}{\sqrt{ab}} \right\} \tag{4.2}$$

y la segunda, la norma también ponderada, de la vectorial euclídea

$$||(x, y, z)||_2 = \sqrt{ax^2 + by^2 + cz^2}. \tag{4.3}$$

[1] Además del procedimiento de Lagrange de reducción, existen otros pocos algoritmos que conducen a la obtención de una primera solución. En [25], artículo de referencia, hay un completo resumen acerca de ellos.

Si (x, y, z) es una solución de (4.1) entonces

$$||(x, y, z)||_2 = \sqrt{2abc}||(x, y, z)||_1 \tag{4.4}$$

por tanto, si las ternas (x, y, z) se restringen a las soluciones de la ecuación (4.1) ambas normas alcanzan valores mínimos en la misma solución.

Se conviene en considerar como solución **pequeña** a aquella (x_o, y_o, z_o) que satisfaga

$$||(x_o, y_o, z_o)||_2 \leq \sqrt{2abc} \tag{4.5}$$

o equivalentemente que $||(x_o, y_o, z_o)||_1 \leq 1$.

Definición 4.1 *Una solución (x_o, y_o, z_o) de la ecuación $ax^2 + by^2 = cz^2$ con a, b, c positivos es pequeña si*

$$ax_o^2 + by_o^2 + cz_o^2 = 2cz_o^2 \leq 2abc \tag{4.6}$$

Esta definición es equivalente a que existe una solución que satisface de forma simultánea estas tres desigueldades

$$|x_o| \leq \sqrt{bc}, \quad |y_o| \leq \sqrt{ac}, \quad |z_o| \leq \sqrt{ab}. \tag{4.7}$$

El teorema de Holzer afirma que existe una solución pequeña. Dice el teorema:

Teorema 4.1 (Teorema de Holzer) *Si la ecuación $ax^2+by^2+cz^2 = 0$ expresada en su forma normal es resoluble, entonces tiene una solución x, y, z no trivial que satisface simultáneamente las cotas,*

$$|x| \leq \sqrt{|bc|}, \quad |y| \leq \sqrt{|ac|}, \quad |z| \leq \sqrt{|ab|}.$$

Estas desigualdades serán además siempre estrictas ya que tanto ab, ac como bc son libres de cuadrados y la raiz nunca es exacta, salvo que dos de los a, b, c sean igual a 1 que son ecuaciones triviales.

Por tanto, de una manera directa, y si los coeficientes de a, b y c no son muy grandes, siempre pueden evaluarse el total $\sqrt{bc}\sqrt{ac}\sqrt{ab}$=$abc$ de ternas que satisfacen las cotas del teorema hasta encontrar una.

Si existe una solución x, y, z con $2cz^2 \leq 2abc$ es decir

$$|z| < \sqrt{|ab|}, \tag{4.8}$$

es inmediato entonces que,

$$|x| = \sqrt{\left|\frac{1}{a}ax^2\right|} < \sqrt{\left|\frac{1}{a}(ax^2+by^2)\right|} = \sqrt{\left|\frac{1}{a}cz^2\right|} < \sqrt{\left|\frac{1}{a}abc\right|} = \sqrt{|bc|}, \quad (4.9)$$

y también de forma similar que,

$$|y| < \sqrt{|ac|},$$

por tanto el teorema será cierto si logramos probar 4.8.

La demostración de 4.8 original de Holzer depende de un resultado sobre números primos en progresión aritmética en un cuerpo cuadrático. Es una demostración que puede considerarse dificil y no generalizable. Además no da un procedimiento constructivo para encontrar esa solución de pequeña magnitud.

Mordell prueba por medios elementales una cotas un poco mas débiles para las soluciones en [13]. Posteriormente en 1969 [18] da otra demostración del teorema de Holzer en la que ofrece un procedimiento para encontrarla. Esta demostración la presenta Mordell en un artículo de apenas dos páginas. Al ser en apariencia más corta, se presupone más sencilla, y lo es en comparación con la original. No obstante en ella da las indicaciones para la demostración sin entrar en los detalles, que no son tan evidentes.

Esta es la demostración exactamente como la publica Mordell. Los detalles se explican en las generalizaciones en los capítulos 6 y 8, ya adaptados a los enteros gausianos y al anillo de polinomios racionales respectivamente:

La idea de la nueva demostración de Mordell permite su implementación algorítmica:

Si una solución (x_o, y_o, z_o) existe con $(x_o, y_o) = 1$ y $|z_o| > \sqrt{ab}$, entonces se puede encontrar otra (x, y, z) con $|z| < |z_o|$.

Pongamos

$$x = x_o + tX, \qquad y = y_o + tY, \qquad z = z_o + tZ$$

donde X, Y, Z son enteros a determinar después. Entonces

$$(aX^2 + bY^2 + cZ^2)t + 2(ax_oX + by_oY + cz_oZ) = 0.$$

De donde, dejando a un lado el denominador, tenemos una solución entera, digamos (x, y, z), dada por

$$\begin{aligned} \delta z &= z_o(aX^2 + bY^2 + cZ^2) - 2Z(ax_oX + by_oY + cz_oZ), \\ \delta x &= x_o(aX^2 + bY^2 + cZ^2) - 2X(ax_oX + by_oY + cz_oZ), \\ \delta y &= y_o(aX^2 + bY^2 + cZ^2) - 2Y(ax_oX + by_oY + cz_oZ), \end{aligned} \tag{4.10}$$

donde δ es un divisor común de las tres expresiones de la derecha.

Probamos que si

$$\delta/c, \qquad \delta/(Xy_o - Yx_o),$$

entonces x, y, z son enteros.

De

$$ax_o^2 + by_o^2 + cz_o^2 = 0,$$

es fácil llegar a que $(\delta, abx_oy_o) = 1$. En (4.10) es suficiente probar que,

$$[P]_\delta = [ax_oX + by_oY]_\delta = [0]_\delta, \qquad [Q]_\delta = [aX^2 + bY^2]_\delta = [0]_\delta.$$

Entonces $[P]_\delta = [Y(ax_o^2 + by_o^2)/y_o]_\delta = [0]_\delta$, ya que $[X]_\delta = [x_oY/y_o]_\delta$.
También $[Q]_\delta = [(ax_o^2 + by_o^2)Y^2/y_o^2]_\delta = [0]_\delta$.

De 4.10 obtengo,

$$\frac{-\delta z}{cz_o} = \left(Z + \frac{ax_oX + by_oY}{cz_o}\right)^2 + \frac{ab}{c^2z_o^2}(y_oX - x_oY)^2. \tag{4.11}$$

Tomo X, Y como cualquier solución de

$$y_oX - x_oY = \delta.$$

Supongo que $z_o^2 > ab$. Primero sea c par. Tomo

$$\delta = \frac{1}{2}c,$$

y Z tal que,

$$\left|Z + \frac{ax_oX + by_oY}{cz_o}\right| \leq \frac{1}{2}.$$

Entonces de (4.11),

$$\frac{1}{2}\left|\frac{z}{z_o}\right| < \frac{1}{4} + \frac{1}{4} \quad \text{y} \quad |z| < |z_o|.$$

Repitiendo este proceso tenemos una solución con $z^2 \leq ab$.

Segundo, sea c impar. Imponemos la condición

$$[aX + bY + cZ]_2 = [0]_2$$

Esto define la paridad de Z. Ya que δ es impar, las tres expresiones de la parte derecha de (4.10) son divisibles por 2δ, y así podemos considerar (4.11) con δ sustituido por 2δ. Tomamos

$$\delta = c,$$

y Z con tal paridad asignada y tenemos

$$\left| Z + \frac{ax_oX + by_oY}{cz_o} \right| \leq 1.$$

Entonces en (4.11) tenemos

$$2\left|\frac{z}{z_o}\right| < 1 + 1 \quad \text{y} \quad |z| < |z_o|.$$

Esto completa la prueba.

Existe otra demostración que se basa en la geometría de números de Cochrane-Mitchel [23] pero, como en la demostración del teroema de Legendre de Davenport y Hall [11] no es generalizable a otros dominios.

5

Los enteros de Gauss

5.1 El dominio euclídeo $\mathbb{Z}[i]$

Un dominio de integridad A es un **dominio euclídeo**, si existe una aplicación N entre los elementos no nulos de A y los naturales satisfaciendo que

1. Si $a, b \in A - \{0\}$ y a divide a b entonces $N(a) \leq N(b)$,

2. **División entera**. Dados $a, b \in A$, $b \neq 0$, existen q y r tales que $a = qb + r$ y con $N(r) < N(b)$ si $r \neq 0$.

A esta aplicación N se le suele llamar **norma euclídea**, y no debemos confundirla con la norma en el sentido clásico vectorial ya que la norma euclídea no necesariamente cumple la desigualdad triangular.

Es conocido que el anillo

$$\mathbb{Z}[i] = \{a + bi : a, b \in Z\}$$

es un dominio euclídeo con la norma el cuadrado del módulo

$$N(a + bi) := a^2 + b^2.$$

(Equivalentemente $N(z) := z\bar{z}$). Esta norma es además multiplicativa

$$N(z_1 z_2) = N(z_1)N(z_2),$$

las unidades de este anillo son $\{1, -1, i, -i\}$ y tenemos que ϵ es unidad si y sólo si $N(z) = 1$.

Un dominio euclídeo es un dominio de factorización única y tendremos, gracias a la división con resto de norma reducida, la posibilidad de escribir cualquier entero de gauss de forma única, salvo producto por una unidad, como un producto de factores gausianos primos. Los teoremas en $\mathbb{Z}$ tienen su versión correspondiente en $\mathbb{Z}[i]$ que también se cumplen.

Existe relación entre la divisibilidad en $\mathbb{Z}$ y $\mathbb{Z}[i]$. Observamos que,

Lema 5.1 *Si z_1 divide a z_2 en $\mathbb{Z}[i]$, entonces $N(z_1)$ divide a $N(z_2)$ en $\mathbb{Z}$.*

Porque si $z_2 = zz_1$ para algún z, entonces $N(z_2) = N(zz_1) = N(z)N(z_1)$ y $N(z_1)$ divide a $N(z_2)$.

En los números primos,

Definición 5.1 *$a+bi$ es primo en $\mathbb{Z}[i]$ si no tiene más divisores que él mismo y las unidades $1, -1, i, -i$.*

sucede que son el mismo número primo $a + bi$ que $\epsilon(a + bi)$, con ϵ unidad. También observamos que,

Lema 5.2 *Si $a + bi$ es un primo gausiano cualquiera, también lo es su conjugado $a - bi$.*

Si z fuese divisor, $a - bi = zz'$ para cierto z', tendríamos $a + bi = \overline{a - bi} = \overline{zz'} = \bar{z}\bar{z}'$, y $\bar{z}$ sería divisor de $a + bi$.

Veamos cómo son los primos.

5.2 Los primos Gaussianos

Antes tenemos que enunciar estos dos teoremas que son resultados clásicos de la teoría de números y que son importantes en la teoría de los enteros de Gauss, los vamos a usar.

Teorema 5.1 *p es un primo del tipo $[p]_4 = [1]_4$ si y sólo si existen enteros u, v tales que de forma única*

$$p = u^2 + v^2.$$

La unicidad y la existencia de esos enteros u, v es clave para clasificar los primos en $\mathbb{Z}[i]$.

Teorema 5.2 *Sea p un primo impar. La ecuación*

$$[x]_p^2 + [1]_p = [0]_p$$

tiene solución si y sólo si p es primo del tipo $[p]_4 = [1]_4$.

que viene a decir que sólo es siempre -1 resíduo cuadrático módulo p cuando p es un primo de la forma $4k + 1$.

En $\mathbb{Z}$ un entero p es primo si es:

el 2,
del tipo $[p]_4 = [1]_4$,
o del tipo $[p]_4 = [3]_4$.

El siguiente teorema resume esencialmente cómo son, y cuáles son los primos en $\mathbb{Z}[i]$.

Teorema 5.3 *Sea el entero gausiano $a + bi$*

(a) *Si a y b son distintos de cero entonces $a + bi$ es primo gausiano si y sólo si $a^2 + b^2$ es primo en $\mathbb{Z}$.*

(b) *Si $b = 0$, entonces a es primo gausiano si y sólo si y $|a|$ es primo en $\mathbb{Z}$ y $[|a|]_4 = [3]_4$.*

(c) *Si $a = 0$, entonces b es primo gausiano si y sólo si y $|b|$ es primo en $\mathbb{Z}$ y $[|b|]_4 = [3]_4$.*

(a) Si $a + bi$ es primo, hemos visto que lo es $a - bi$. Si $N(a + bi)$ no fuese primo en $\mathbb{Z}$ tiene entonces un divisor $1 < d < N(a + bi)$ el cual, dado que $N(a + bi) = (a + bi)(a - bi)$ dividiría a $a + bi$ o a $a - bi$ lo que no es posible por ser ambos primos. Recíprocamente, sea $N(a + bi)$ primo en $\mathbb{Z}$, si $a + bi$ no fuese primo se podría factorizar no trivialmente

$$a + bi = (c + di)(e + fi)$$

y entonces

$$a^2 + b^2 = N(a + bi) = N((c + di)(e + fi)) = (c^2 + d^2)(e^2 + f^2)$$

sería una factorización no trivial de $a^2 + b^2$ lo que es contradicción.

(b) Si $|a|$ es entero primo sin divisores triviales en $\mathbb{Z}[i]$, tampoco los tiene a y tampoco los puede tener a en $\mathbb{Z}$. Recíprocamente si a, con $[|a|]_4 = [3]_4$ primo en $\mathbb{Z}$, no fuese primo en $\mathbb{Z}[i]$, se factorizaría

$$|a| = (c + di)(e + fi)$$

y entonces

$$N(|a|) = N(a) = a^2 = N((c + di)(e + fi)) = (c^2 + d^2)(e^2 + f^2)$$

con lo que al tratarse de enteros, necesariamente

$$a = c^2 + d^2 = e^2 + f^2$$

lo que no puede ser posible por el teorema 5.1.

(c) Es inmediato ya que en $\mathbb{Z}[i]$, a es primo si y sólo si lo es ai.

Del teorema se sigue que salvo producto por unidades y conjugados $1+i$, $1+2i$, 3, $2+3i$, 7, $2+5i\ldots$ son primos gausianos y $2, 5, 13, 17\ldots$ no lo son.

5.3 Las clases residuales $\mathbb{Z}[i]_{a+bi}$

En los enteros, el número de clases módulo n es la cantidad de enteros no negativos con menor módulo que n, que son

$$[0]_n, [1]_n, [2]_n, \cdots, [n-1]_n.$$

En los enteros de Gaus el número de clases de $a + bi$ no es la cantidad de gausianos con módulo menor. Dos de ellos con menor módulo pueden ser congruentes entre si. Por ejemplo $[i]_{1+2i} = [2]_{1+2i}$ ya que $i - 2 = i(1 + 2i)$.

Veamos cuántas clases hay y de qué forma podemos elegir una representación de sus clases.

Teorema 5.4 *El número de clases módulo un primo $a + bi$ es $a^2 + b^2$.*

Vamos que cualquier $c + di$ es congruente módulo $a + bi$ con algunos de los $a^2 + b^2$ enteros

$$0, 1, 2, \cdots, a^2 + b^2 - 1.$$

Supongamos que $a+bi$ es primo del tipo descrito en el teorema 5.3 (a). Al ser $\gcd(b, a^2+b^2) = 1$ existe el inverso $[1/b]_{a^2+b^2}$. $1/b$ es entero múltiplo de a^2+b^2 por tanto también lo es de $a+bi$. Existe pues siempre un representante entero del inverso de b módulo $a+bi$,

$$[1/b]_{a^2+b^2} = [1/b]_{a+bi}$$

puedo entonces de $[a+bi]_{a+bi} = [0]_{a+bi}$, despejar $[i]_{a+bi} = [-a/b]_{a+bi}$ y sustituir en $c+di$

$$[c+di]_{a+bi} = [c - d\frac{a}{b}]_{a+bi}$$

con lo que $c - d\frac{a}{b}$ es un representante de clase entero de $c+di$ módulo $a+bi$. Como a lo sumo existen a^2+b^2 valores distintos para $c - d\frac{a}{b}$, ya que a^2+b^2 es múltiplo de $a+bi$, entonces cada $c+di$ es congruente con algún entero $0, 1, 2, \cdots, a^2+b^2-1$ módulo $a+bi$. Como además estos números no son congruentes nunca entre si ya que si fuera $[r]_{a+bi} = [s]_{a+bi}$ con $0 \leq r < s < a^2+b^2$, entonces $a+bi$ divide a $r-s$, también la norma $N(a+bi) = a^2+b^2$ divide a $N(r-s)^2 = (r-s)^2$ y como a^2+b^2 es primo, divide a $r-s$ lo que sólo es posible si $r = s$. Por lo tanto,

$$\{[0]_{a+bi}, [1]_{a+bi}, [2]_{a+bi}, \cdots, [a^2+b^2-1]_{a+bi}\}$$

es un conjunto completo de representantes de clase, con a^2+b^2 representantes enteros, módulo $a+bi$.

Por último supongamos que $a+bi$ es un primo del tipo descrito en el teorema 5.3 (b). Tenemos $b = 0$ y a con $[a]_4 = [3]_4$. Veamos que el conjunto

$$\{r+si : 0 \leq r, s < a\}$$

que tiene a^2 elementos, es un conjunto completo de representantes de clase. Cualquiera que fuera $c+di$, se tiene que

$$[c+di]_a = [c]_a + [di]_a = [r]_a + [si]_a = [r+si]_a$$

para ciertos r, s, con $0 \leq r, s < a$. Además son todos incongruentes ya que si fuese $[r+si]_a = [t+ui]_a$ entonces $[(r-t)+(s-u)i]_a = [0]_a$ y como $0 \leq r, s, t, u < a$, esto sólo es poisible si $r = t$ y $s = u$.

El teorema está probado.

Consideremos la función n,

$$n(z) := \text{número de clases módulo } z,$$

esta función es multiplicativa:

Teorema 5.5 *Si x, y son gaussianos no nulos, entonces*

$$n(xy) = n(x)n(y).$$

Sean

$$x_1, x_2, \cdots, x_i, \cdots x_{n(x)} \qquad y_1, y_2, \cdots, y_j, \cdots y_{n(y)}$$

dos conjuntos de representantes completos de clase de x e y. Sea cualquier entero gausiano z. Entonces $[z]_x = [x_i]_x$ para algún i, luego $z - x_i = xr$ para cierto gausiano r. A su vez $[r]_y = [y_j]_y$ para algún j. Tenemos $r - y_j = sy$ para cierto gausiano s. Sustituimos y tenemos

$$z = x_i + xr = x_i + x(y_j + sy) = x_i + xy_j + sxy$$

es decir que $[z]_{xy} = [x_i + xy_j]_{xy}$ y entonces los xy gausianos $x_i + xy_j$ son un conjunto de representantes de $\mathbb{Z}[i]_{xy}$. Veamos que es completo sin repeticiones. Para ello supongamos que tenemos

$$[x_i + xy_j]_{xy} = [x_{i'} + xy_{j'}]_{xy} \tag{5.1}$$

y probemos que $i = i'$ y que $j = j'$. Tomamos clases módulo x en (5.1) tenemos

$$[x_i]_x = [x_i + xy_j]_x = [x_{i'} + xy_{j'}]_x = [x_{i'}]_x$$

luego necesariamente $i = i' = k$. Restando ambos miembros de la igualdad (5.1) tenemos

$$[x_k + xy_j]_{xy} - [x_k + xy_{j'}]_{xy} = [xy_j - xy_{j'}]_{xy} = [0]_{xy}$$

que implica $[y_j - y_{j'}]_y = [0]_y$, luego $j = j'$.

Teniendo en cuenta el teorema 5.4 y que todo entero gausiano puede ser descompuesto en producto de factores primos ya que $\mathbb{Z}[i]$ es un dominio de factorización única, entonces tenemos,

Teorema 5.6 *El número de clases módulo cualquier gausiano $a + bi$ es $a^2 + b^2$.*

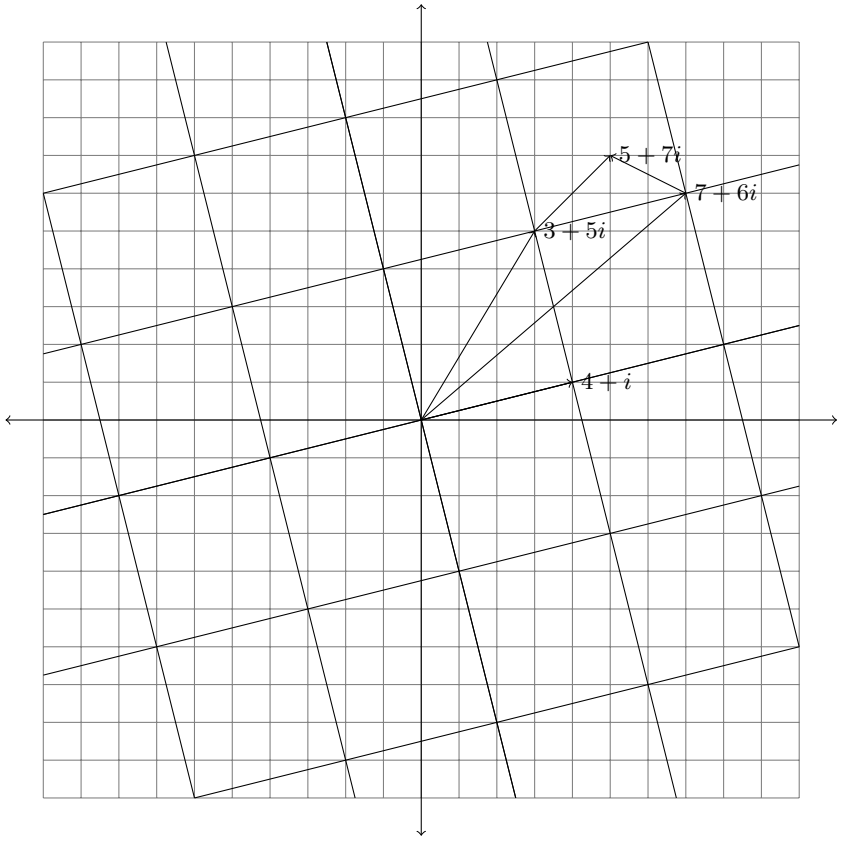
5.4 Los múltiplos gausianos

Si observamos que un múltiplo gaussiano de $a + bi$ cualquiera, pongamos que sea $(c + di)(a + bi)$, puede ser expresado como una combinación

$$c\,(a + bi) + d\,i(a + bi)$$

de $a + bi$ y de $i(a + bi)$ siendo este segundo, justamente el primero girado noventa grados, entonces gráficamente ese múltiplo de $a + bi$ es la suma de c veces $a + bi$ con d veces $i(a + bi)$ que está en dirección perpendicular. Todos los múltiplos estarían así dispuestos de manera que formarían una cuadrícula de arista $\sqrt{a^2 + b^2}$, el módulo de $a + bi$, y de diámetro $\sqrt{2}\sqrt{a^2 + b^2}$.

En la figura,



tenemos a los múltiplos de $4+i$ en los vértices de dicha cuadrícula. Podemos ver que $7 + 6i$ es un multiplo porque es dos veces $4 + i$ más una vez $4 + i$ girado noventa grados, es decir $7 + 6i = (2 + i)(4 + i)$.

En la división de p entre q en $\mathbb{Z}$, $p = Mq+r$, como p entero tiene a ambos lados de él, y sobre una línea a dos múltiplos del divisor q, puede elegirse el múltiplo más próximo a p de manera que el resto r en valor absoluto sea menor que $\frac{1}{2}|q|$. El resto puede ser positivo o negativo. Decimos con resto por exceso o por defecto.

En $\mathbb{Z}[i]$, p dispone de los cuatro múltiplos de q más próximos, que le rodean a elegir para la division por q. Con al menos uno de ellos, el resto será con módulo menor o igual que $\frac{\sqrt{2}}{2}|q|$, o equivalentemente con norma menor o igual que $\frac{1}{2}N(q)$.

Esto es geométricamente inmediato. La demostración del teorema proporciona un método constructivo para encontrar ese resto.

Teorema 5.7 *Sean p y q enteros Gausianos, entonces existe al menos un entero gausiano r, tal que $[r]_q = [p]_q$ con*

$$N(r) \leq \frac{\sqrt{(2)}}{2}|q| = \frac{1}{2}N(q)$$

Sea

$$\frac{p}{q} = x + yi$$

la división de p y q en los racionales gausianos $\mathbb{Q}[i]$. Sean a, b los enteros más próximos a los racionales x, y. Tendremos,

$$|x - a| \leq \frac{1}{2} \quad \text{y} \quad |y - b| \leq \frac{1}{2}.$$

Elegimos entonces el múltiplo

$$(a + bi)\, q$$

y su resto $r = p - (a + bi)\, q$ satisface,

$$\begin{aligned} N(r) = N\left(q(p/q - (a + bi))\right) &= N(q)N(x - a + (y - b)i) \\ &\leq N(q)(\frac{1}{4} + \frac{1}{4}) = \frac{1}{2}N(q). \end{aligned}$$

En la figura, vemos que $5 + 7i$ puede dividirse por $4 + i$ con los cuatro múltiplos que le rodean, en particular

$$5 + 7i = (2 + i)(4 + i) + (-2 + i), \quad 5 + 7i = (1 + i)(4 + i) + (2 + 2i)$$

con restos $-2+i$, $2+2i$ con módulos ambos menores que $\frac{\sqrt{2}}{2}\sqrt{17}$.

5.5 La ecuación de Legendre en $\mathbb{Z}[i]$

En la demostración del teorema tal y como lo presenta en su artículo Samet da las indicaciones sin entrar en detalles para la prueba de un lema que parece evidente y es necesario.

A continuación se presenta una demostración completa detallada del teorema de Legendre en $\mathbb{Z}[i]$.

Teorema 5.8 (de Legendre en los enteros de Gauss) *La condición necesaria y suficiente para que la ecuación*

$$ax^2 + by^2 + cz^2 = 0 \tag{5.2}$$

satisfaciendo

(i) *a, b, c libre de cuadrados*

(ii) *a, b, c primos dos a dos*

tenga solución no trivial en los enteros Gausianos, es que

(iii) *bc, ac, ab sean residuos cuadrádricos de a, b y c respectivamente.*

La condición es siempre necesaria. Repetimos de nuevola prueba ahora en $\mathbb{Z}[i]$.

Supongamos que la ecuación tiene solución primitiva (x_o, y_o, z_o). Necesariamente $\gcd(x_o, y_o) = \gcd(x_o, z_o) = \gcd(y_o, z_o) = 1$, ya que si fuese $\gcd(x_o, y_o) \neq 1$ tendríamos $x_o = px'$, $y_o = py'$ con p primo común con $-cz_o^2 = a(px')^2 + b(py')^2$, y entonces $[-cz_o^2]_{p^2} = [p^2]_{p^2}[ax'^2 + by'^2]_{p^2} = [0]_{p^2}$ lo que no es posible ya que p no divide a z_o y p^2 no o hace a z_o^2, y tampoco p^2 divide a c que está libre de cuadrados. Además $\gcd(x_o, c) = 1$, ya que si p fuera un primo común debería dividir a by_o^2, no lo hace a b por ser b, c primos entre si, y no lo hace a y_o^2 ni a y_o por ser x_o e y_o primos entre si.

Al ser $ax_o^2 + by_o^2 = -cz_o^2$ entonces $[ax_o^2 + by_o^2]_c = [0]_c$ y multiplicando por $[(1/x_o)^2 b]_c$ se tiene $[ab + b^2 y_o^2 (1/x_o)^2]_c = [0]_c$. Por tanto

$$[(by_o/x_o)^2]_c = [-ab]_c = [i^2 ab]_c$$

y según el teorema 2.4 como $(i, c) = 1$, ab es también residuo cuadrático de c. De forma semejante se prueba que bc, ac son también residuos cuadráticos de a y b respectivamente. Esto prueba la necesidad.

Sea la ecuación de Legendre en los enteros de Gauss en su forma normal con sus coeficientes ordenados de manera que $|a| \leq |b| \leq |c|$.

Definición 5.2 *El* **índice** *de esta ecuación es el valor mediano* $|ac|$ *de la sucesión* $|ab| \leq |ac| \leq |bc|$

En este anillo de los enteros de Gauss el índice no es necesariamente un número entero. Si lo es su cuadrado. Antes de abordar la demostración de la suficiencia probamos el lema,

Lema 5.3 *Sean a, b, c, enteros gausianos libres de cuadrados y primos dos a dos. Si* $|a| = |b| = |c|$ *entonces* a, b, c *son unidades, es decir*

$$|a| = |b| = |c| = 1.$$

Al absurdo, supongamos que $|a| = |b| = |c| \neq 1$, entonces

$$N(a) = N(u + iv) = u^2 + v^2$$

es divisible por algún entero primo p. Según el tipo de primo del que se trate en los enteros tenemos,

Si el primo fuera $p = 2$:

Los enteros u, v serían ambos pares e impares. Si fueran pares, 2 dividiría a a y como $2 = (1 + i)(1 - i)$, también $1 + i$ divide a a. Si fueran impares,

$$(u + 1) + i(v + 1) = a + (1 + i)$$

es divisible por 2 y por tanto por $1+i$, también debe ser entonces a divisible por $1 + i$.

En ambos casos a sería divisible por $1 + i$. Llegaríamos a la misma conclusión con b y con c, lo que es contradicción porque a, b, c son primos dos a dos.

Si el primo fuera del tipo $[p]_4 = [3]_4$:

Si $[v]_p \neq [0]_p$, v es inversible en $\mathbb{Z}_p$, y $[u/v]_p$ satisface

$$[u/v]_p^2 + [1]_p = [(u^2 + v^2)/v^2]_p = [0]_p$$

lo que es imposible por el teorema 5.2, por lo tanto $[v]_p = [0]$ y entonces p divide a u^2 y a u, por tanto lo hace a $u + iv$. Llegaríamos a la misma conclusión con b y con c, lo que es contradicción porque a, b, c son primos dos a dos.

Si el primo fuera del tipo $[p]_4 = [1]_4$:

Según el teorema 5.1 existen s, t con

$$p = s^2 + t^2 = (s + it)(s - it).$$

Veamos entonces que alguno de $s + it$, $s - it$ divide a a.

Si p divide a v, entonces como antes, p divide a u^2 y a u, lo hace a $u+iv$, y por tanto ambos $s + it$ y $s - it$ dividen a $a = u + iv$.

Si $[v]_p \neq [0]_p$, como $[(u/v)^2 + 1]_p = [(u^2 + v^2)/v^2]_p = [0]_p$ y también $[(s/t)^2 + 1]_p = [(s^2 + t^2)/t^2]_p = [0]_p$, restando entonces,

$$[(s/t)^2 - (u/v)^2]_p = [s/t + u/v]_p[s/t - u/v]_p = [0]_p$$

por lo que $[u/v]_p = [s/t]_p$ o bien $[u/v]_p = -[s/t]_p$. En el primer caso si tomamos $k = [u/s]_p = [v/t]_p$ y escribimos $[u]_p = [ks]_p$, $[v]_p = [kt]_p$, al ser $[u - ks]_p = [0]_p$ y $[v - kt]_p = [0]_p$ sumamos y concluímos que

$$[u - ks + i(v - kt)]_p = [u + iv - k(s + it)]_p = [0]_p$$

por tanto $[u + iv]_p = [k(s + it)]_p$ y $s + it$ divide a $a = u + iv$. De forma análoga concluímos en el segundo caso que $s - it$ divide a a.

Como esto puede hacerse también para b y para c, al menos dos de los tres tendrá un divisor común $s + it$ o $s - it$. Lo que es contradicción por ser a, b, c primos dos a dos. Esto prueba el lema.

Por tanto en la ecuación una de las desigualdades de

$$|a| \leq |b| \leq |c|, \tag{5.3}$$

es siempre estricta. Probamos ahora el teorema.

Consideremos la ecuación de Legendre en su forma normal ordenada. Procedemos por inducción sobre el índice $J = |ac|$ de las ecuaciones. Probamos que el teorema es cierto para $J = 1$ y suponiendo cierto el teorema para ecuaciones de índice menor que J probamos que lo es para los de índice J [1].

[1] Los valores al cuadrado de los índices J^2 forman una sucesión de enteros positivos

Si el índice es $|ac| = 1$, entonces $|a| = |b| = |c| = 1$, las ecuaciones que satisfacen las condiciones del teorema son alguna de

$$x^2 + y^2 + \epsilon z^2 = 0 \qquad \text{ó} \qquad x^2 - y^2 + \epsilon z^2 = 0$$

con ϵ unidad, que tienen solución $(1, i, 0)$ y $(1, 1, 0)$.

Probado el caso $J = 1$, supongamos $J > 1$.

Según la condición del teorema 5.8(iii), existe R entero gaussiano con

$$[R^2]_c = [ab]_c.$$

Como $\gcd(a, c) = 1$ podemos dividir por a^2 y tenemos $[r^2]_c = [(R/a)^2]_c = [b/a]_c$. Tomemos r con $N(r) \leq \frac{1}{2}N(c)$, es decir

$$|r| \leq \frac{1}{\sqrt{2}}|c|$$

cosa que es siempre posible por el teorema 5.7.

Por tanto $[ar^2]_c = [b]_c$ y podemos concluir que para cierto Q,

$$ar^2 - b = cQ. \tag{5.4}$$

Si Q es 0, entonces $ar^2 = b$ y como b es libre de cuadrados, necesariamente $|r| = 1$, lo que nos lleva a que $a = \pm b$, y por ser $\gcd(a, b) = 1$, salvo unidades, la ecuación es alguna de

$$x^2 + y^2 + cz^2 = 0 \qquad \text{ó} \qquad x^2 - y^2 + cz^2 = 0,$$

que tienen siempre solución respectivamente

$$1, i, 0, \quad 1, 1, 0.$$

Por tanto salvo este caso, en el que el teorema ya se cumple, podemos considerar que Q es distinto de cero.

Sea A el máximo común divisor de los tres términos de la ecuación (5.4). Como A divide a b, A es primo relativo a a y c, por tanto A divide necesariamente a r^2 y a Q. Como el divisor A de b no puede tener factores cuadrados por no tenerlos b, entonces A divide a r.

$j_1, j_2, \cdots, j_n, \cdots$. Probamos que el teorema es cierto para $J = 1$, y que si lo es para $J^2 \leq j_n$ entonces lo es para $J^2 \leq j_{n+1}$.

Podemos poner entonces

$$r = A\alpha, \qquad b = A\beta, \qquad Q = Aq = AC\gamma^2 \tag{5.5}$$

donde γ^2 es el mayor cuadrado que divide a q. Sustituyo en (5.4), simplifico y obtengo

$$aA\alpha^2 - \beta = cC\gamma^2. \tag{5.6}$$

Sea $B = a\beta$ y consideremos la ecuación

$$AX^2 + By^2 + CZ^2 = 0. \tag{5.7}$$

Veamos que si $J > 2$, el índice de (5.7) es menor que J y podremos aplicar la hipótesis de inducción. Antes probemos el teorema para los casos que faltan, $J = \sqrt{2}$ y $J = 2$.

Caso $|ac| = J = \sqrt{2}$:

En un principio $a = \epsilon_1$, $b = \epsilon_2$ ó $\epsilon_2(1+i)$, $c = \epsilon_3(1+i)$ con ϵ_1, ϵ_2, ϵ_3 unidades. Pero $b = \epsilon_2(1+i)$ no es posible porque b y c son coprimos. En los casos restantes, multipliquemos c por la unidad conveniente para que sea igual a $(1+i)$ y entonces para $\epsilon_1 = \epsilon_2$ la solución es $(1, i, 0)$, y para $\epsilon_1 = 1$, $\epsilon_2 = i$ la solución es $(1, 1, i)$. Los demás son permutaciones y cambios de signo en los coeficientes a, b de los dos casos anteriores que también tienen entonces solución.

Caso $|ac| = J = 2$:

No hay ecuación de índice 2, ya que si $|ac| = 2$ o bien $|a| = |c| = \sqrt{2}$ lo que obliga a que $|b| = \sqrt{2}$ con lo que habría de ser $a = 1+i$, $1-i$ cosa no posible por ser a, b primos entre si, o bien $|a| = 1$, $|c| = 2$ que también es imposible porque c tendría el cuadrado $(1+i)^2 = 2$ contradiciendo las condiciones del teorema.

Caso $|ac| = J > 2$:

Despejamos Q de (5.4) y tenemos que

$$|AC| \leq |AC\gamma^2| = |Q| \leq \frac{|ar^2| + |b|}{|c|} \leq \frac{1}{2}|ac| + \frac{|b|}{|c|} = \frac{1}{2}J + 1 < J$$

también

$$|AB| = |\frac{b}{\beta}a\beta| = |ab| \leq J \tag{5.8}$$

Luego el índice de la reducida es $\leq J$.

En el caso en que $|a| \leq |b| < |c|$ entonces $|AB| = |ab| < |ac| = J$, y cualquiera que sea el valor de $|BC|$ el índice de (5.7) es $< J$.

Y en el caso en que $|a| < |b| = |c|$, entonces si el índice no fuese $< J$, es que se tiene $|AC| < J = |ab| = |AB| \leq |BC|$, es decir

$$|A| \leq |C| < |B|$$

y volviendo a aplicar el proceso de reducción a la ecuación $AX^2 + CY^2 + BZ^2 = 0$ que está en el caso anterior nos da una de índice $< J$.

Antes de aplicar la hipótesis de inducción veamos que la ecuación (5.7) satisface las condiciones del teorema.

Es evidente que ninguno de A, B, C es cero.

Como a, b son primos relativos y libre de cuadrados; $AB = ab$ implica que también A y B son primos relativos y libres de cuadrados.

Como γ^2 es el mayor cuadrado que divide a $q = C\gamma^2$, C no tiene factores cuadrados. Y como los términos de (5.6) son primos dos a dos, C es primo a $aA\beta = AB$. Estos prueba (i) y (ii).

Teniendo en cuenta (5.6), cuyos términos son primos dos a dos, aplicamos el teorema 2.4 y tenemos que, βcC es resíduo cuadrático de aA, $acAC$ es resíduo cuadrático de β, y $aA\beta = AB$ es resíduo cuadrático de C.

Por hipótesis, $bc = \beta Ac$ es residuo cuadrático de a, y ac lo es de $b = A\beta$ y por tanto de A. Ya que βcC y ac son residuos cuadráticos de A, también el producto de los dos $\beta cCac = BCc^2$ y por tanto BC es resíduo cuadrático de A.

Como ac y $acAC$ son residuos cuadráticos de β, lo es el producto a^2c^2AC y lo es AC. Sea u con $[u^2]_\beta = [AC]_\beta$. Como βcC y βAc y su producto β^2c^2AC y AC son residuos cuadráticos de a, sea v con $[v^2]_a = [AC]_a$. Como los términos de 5.6 son primos dos a dos también lo son a y β. Por el teorema chino del resto existe una solución w común con $[w]_\beta = [u]_\beta$, $[w]_a = [v]_a$. Por tanto $w^2 - AC$ es divisible por β y a y por $\beta a = B$. Luego AC es residuo cuadrático de B. Esto prueba (iii).

Aplicamos ahora la hipótesis de indución. Sea (X, Y, Z) una solución de (5.7), y pongamos

$$\begin{aligned} x &= A\alpha X - i\beta Y \\ y &= iX + a\alpha Y \\ z &= C\gamma Z \end{aligned} \tag{5.9}$$

por 5.5 y 5.6 y la definición de $B = a\beta$, resulta

$$ax^2 + by^2 + cz^2 = cC\gamma^2(AX^2 + BY^2 + CZ^2) = 0$$

por lo que (x, y, z) es solución de 5.2.

La solución obtenida no es la trivial.
Si fuera, $x = y = 0$, eliminando X nos da

$$(-\beta + Aa\alpha^2)Y = 0.$$

Como el primer factor no es cero por 5.6 necesariamente $Y = 0$. También lo serían

$$X = \frac{1}{i}y = 0, \quad \text{y} \quad Z = 0,$$

lo que es falso. Esto completa la demostración.

6

El teorema de Holzer en $\mathbb{Z}[i]$

Si consideramos en $\mathbb{Z}[i]^3$ la norma definida mediante el módulo,

$$||(x, y, z)|| = \sqrt{|ax^2| + |by^2| + |cz^2|},$$

que generaliza a la anteriormente dada $|| \cdot ||_2$ en el capítulo 4 en $\mathbb{Z}^3$, y definimos también como solución pequeña como aquella que satisface

$$|ax^2| + |by^2| + |cz^2| \leq 2|abc|,$$

no podemos asegurar que exista siempre una solución pequeña en la ecuación $ax^2 + by^2 + cz^2 = 0$ en $\mathbb{Z}[i]$.

El enunciado del teorema de Holzer en los enteros de Gauss, si sustituímos el valor absoluto por el módulo del complejo no se cumple tampoco, es decir no tiene porqué existir siempre una solución (x, y, z) que satisface simuláneamente las tres desigualdades

$$|x| \leq \sqrt{|bc|}, \quad |y| \leq \sqrt{|ac|}, \quad |z| \leq \sqrt{|ab|}.$$

Por ejemplo, la ecuación

$$ix^2 + 7y^2 + z^2 = 0$$

tiene como solución más pequeña a $(2 + 2i, 1, 1)$ en donde

$$|(2 + 2i)^2| + |7| + |1| = 16,$$

pero $2|abc| = 14$. En cuanto a las tres desigualdades simultáneas, no la

cumple x,

$$|x| = |2 + 2i| = \sqrt{8} > \sqrt{|bc|} = \sqrt{|7|}.$$

Pero pueden modificarse las cotas de Holzer para enunciar el teorema en $\mathbb{Z}[i]$. Adaptando la demostración de Mordell [18] probamos que al menos se cumple el siguiente teorema:

Teorema 6.1 *La ecuación*

$$ax^2 + by^2 + cz^2 = 0 \tag{6.1}$$

en $Z[i]$ expresada en su forma normal, si tiene soluciones, entonces tiene una (x, y, z) con

$$|z| \leq \sqrt{(1 + \sqrt{2})|ab|}.$$

La demostración consistirá también en probar que si existe una solución (x_o, y_o, z_o) con $(x_o, y_o) = 1$ y $|z_o| > \sqrt{(1 + \sqrt{2})|ab|}$, se puede encontrar a partir de ella otra (x, y, z) con $|z| < |z_o|$.

Parametrizamos las soluciones imponiendo que

$$(x_o + tX, y_o + tY, z_o + tZ) \tag{6.2}$$

sea una solución en los racionales de Gauss con X, Y, Z parámetros enteros gausianos y t racional gausiano, $t \neq 0$. Sustituimos en (6.1) y obtengo

$$\begin{aligned} 0 = a(x_o + tX)^2 + b(y_o + tY)^2 + c(z_o + tZ)^2 = \\ ax_o^2 + 2ax_otX + at^2X^2 + by_o^2 + 2by_otY + bt^2Y^2 + cz_o^2 + 2cz_otZ + ct^2Z^2 = \\ ax_o^2 + by_o^2 + cz_o^2 + (aX^2 + bY^2 + cZ^2)t^2 + 2t(ax_oX + by_oY + cz_oZ) = \\ t((aX^2 + bY^2 + cZ^2)t + 2(ax_oX + by_oY + cz_oZ)). \end{aligned}$$

Ya que $t \neq 0$, obtengo

$$t = \frac{-2(ax_oX + by_oY + cz_oZ)}{aX^2 + bY^2 + cZ^2}$$

que sustituido en (8.4) nos da las soluciones en los racionales de Gaus de

6.1, multiplicando por $aX^2+bY^2+cZ^2$ obtengo las soluciones enteras

$$\begin{aligned} x_o(aX^2+bY^2+cZ^2)-2X(ax_oX+by_oY+cz_oZ)\\ y_o(aX^2+bY^2+cZ^2)-2Y(ax_oX+by_oY+cz_oZ)\\ z_o(aX^2+bY^2+cZ^2)-2Z(ax_oX+by_oY+cz_oZ)\end{aligned} \tag{6.3}$$

que podemos simplificar por un divisor común δ de las tres expresiones de 8.5, no necesariamente el máximo común divisor, de manera que tendremos una solución (x,y,z) dada por

$$\begin{aligned} x&=\frac{1}{\delta}(x_o(aX^2+bY^2+cZ^2)-2X(ax_oX+by_oY+cz_oZ))\\ y&=\frac{1}{\delta}(y_o(aX^2+bY^2+cZ^2)-2Y(ax_oX+by_oY+cz_oZ))\\ z&=\frac{1}{\delta}(z_o(aX^2+bY^2+cZ^2)-2Z(ax_oX+by_oY+cz_oZ)).\end{aligned} \tag{6.4}$$

Probamos ahora que si

$$\delta \text{ divide a } c, \text{ y divide a } Xy_o-Yx_o,$$

entonces divide a las tres expresiones de (6.3) y en consecuencia (x,y,z) son enteros. Para ello previamente veamos que a, b, x_o y y_o son inversibles en el anillo $Z[i]_\delta$. Será suficiente ver que $\gcd(\delta, abx_oy_o)=1$. Supongamos que existiese un primo p divisor común de δ y de abx_oy_o. Como $\delta|c$ y a, b, c son primos entre si entonces p sólo podría dividir a x_oy_o. Supongamos que lo hace a x_o. Como $ax_o^2=-by_o^2-cz_o^2$ y como p no divide a b, debe hacerlo a y_o^2 y en consecuencia a y_o lo que es una contradicción porque $\gcd(x_o,y_o)=1$.

Ahora, puesto que δ divide a Xy_o-Yx_o, entonces $[Xy_o-Yx_o]_\delta=[0]_\delta$. Si despejo $[X]_\delta=[Yx_o/y_o]_\delta$, y sustituyo en $[aX^2+bY^2+cZ^2]_\delta$ y en $[ax_oX+by_oY+cz_oZ]_\delta$

$$\begin{aligned} [a(Yx_o/y_o)^2+bY^2+cZ^2]_\delta=\left[(ax_o^2Y^2+byo^2Y^2+cy_o^2Z^2)/y_o^2\right]_\delta=\\ =\left[(-cz_o^2Y^2+cy_o^2Z^2)/y_o^2\right]_\delta=[c]_\delta\left[(-z_o^2Y^2+y_o^2Z^2)/y_o^2\right]_\delta=[0]_\delta\\ [(ax_o(Yx_o/y_o)+by_oY+cz_oZ]_\delta=\left[(ax_o^2Y+byo^2Y+cy_o^2Z)/y_o\right]_\delta=\\ =\left[(-cz_o^2Y+cy_o^2Z)/y_o\right]_\delta=[c]_\delta\left[(-z_o^2Y+y_o^2Z)/y_o\right]_\delta=[0]_\delta,\end{aligned}$$

obtenemos múltiplos de δ por serlo c. Por tanto las expresiones de (6.3) también son múltiplos de δ, y (x,y,z) es solución entera.

Manipulamos la ecuación (6.4) para poder comparar z con z_o:

$$\begin{aligned}\frac{-\delta z}{cz_o} &= \frac{2Z(ax_oX + by_oY + cz_oZ)}{cz_o} - \frac{z_o(aX^2 + bY^2 + cZ^2)}{cz_o} \\ &= Z^2 + 2Z(\frac{ax_oX + by_oY}{cz_o}) - \frac{aX^2 + bY^2}{c} \\ &= (Z + \frac{ax_oX + by_oY}{cz_o})^2 - (\frac{ax_oX + by_oY}{cz_o})^2 - \frac{aX^2 + bY^2}{c} \\ &= (Z + \frac{ax_oX + by_oY}{cz_o})^2 \\ &\quad - \frac{1}{c^2z_o^2}(aX^2cz_o^2 + bY^2cz_o^2 + a^2x_o^2X^2 + b^2y_o^2Y^2 + 2abx_oy_oXY)\end{aligned}$$

como $cz_o^2 = -ax_o^2 - by_o^2$,

$$\begin{aligned}&= (Z + \frac{ax_oX + by_oY}{cz_o})^2 + \frac{ab}{c^2z_o^2}(y_o^2X^2 - 2x_oy_oXY + x_o^2Y^2) \\ &= (Z + \frac{ax_oX + by_oY}{cz_o})^2 + \frac{ab}{c^2z_o^2}(y_oX - x_oY)^2\end{aligned}$$

y obtenemos

$$z = z_o\frac{-c}{\delta}\left[(Z + \frac{ax_oX + by_oY}{cz_o})^2 + \frac{ab}{c^2z_o^2}(y_oX - x_oY)^2\right]. \tag{6.5}$$

Como $gcd(x_o, y_o) = 1$ la ecuación $y_oX - x_oY = \delta$ siempre tiene solución. Para nuestro propósito escogeremos los valores de X, Y, Z según si c es múltiplo o no de $(1 + i)$ como sigue:

Si c es múltiplo de $1 + i$, podemos tomar

$$\delta = \frac{1}{1+i}c,$$

tomar los parámetros X, Y como una solución cualquiera de

$$y_oX - x_oY = \frac{1}{1+i}c$$

y el valor de Z como el entero gausiano más próximo al racional gausiano

$$-\frac{ax_oX + by_oY}{cz_o}.$$

Siendo así, se tiene

$$\left| Z + \frac{ax_oX + by_oY}{cz_o} \right| < \frac{\sqrt{2}}{2}.$$

Esto es así porque geométricamente los enteros gaussianos se encuentran situados en una cuadrícula de arista igual a 1 y diámetro $\sqrt{2}$. Cualquier racional de Gauss que se encuentre dentro de un cuadrado distaría de un entero de Gauss a lo sumo la mitad del diámetro.

Supongamos que

$$|z_o| > \sqrt{(1+\sqrt{2})|ab|},$$

tomando módulos en (6.5)

$$|z| = |z_o||1+i| \left| (Z + \frac{ax_oX + by_oY}{cz_o})^2 + \frac{(1+\sqrt{2})ab}{(1+\sqrt{2})(1+i)^2 z_o^2} \right| <$$
$$< |z_o|\sqrt{2} \left((\frac{\sqrt{2}}{2})^2 + \frac{1}{(1+\sqrt{2})(\sqrt{2})^2} \right) = |z_o|\sqrt{2}\frac{2+\sqrt{2}}{2+2\sqrt{2}} = |z_o|.$$

Si c no es múltiplo de $1+i$, escogemos X e Y cualquier solución de $y_oX - x_oY = c$. Como $Z[i]_{1+i} = \{[0]_{1+i}, [1]_{1+i}\}$, si Z satisfaciera la ecuación

$$[aX + bY + cZ]_{1+i} = [0]_{1+i} \tag{6.6}$$

entonces las expresiones (6.3) también son divisibles por $1+i$, ya que lo es $aX^2+bY^2+cZ^2$ porque cualquiera que sea α en $Z[i]$ se tiene $[\alpha^2]_{1+i} = [\alpha]_{1+i}$, y entonces

$$[aX^2 + bY^2 + cZ^2]_{1+i} = [aX + bY + cZ]_{1+i} = [0]_{1+i}$$

y además también lo es $2 = (1+i)(1-i)$. De esta forma se establece la paridad de Z que es o bien múltiplo de $1+i$ o bien 1 más múltiplo de $i+1$. Escojamos pues Z como el entero gausiano con esa paridad que sea más próximo a $-\frac{ax_oX+by_oY}{cz_o}$ y tendremos que

$$\left| Z + \frac{ax_oX + by_oY}{cz_o} \right| < 1$$

porque los múltiplos de $1+i$ y los que no, se encuentran situados en una cuadrícula de arista $\sqrt{2}$ y de diámetro $((\sqrt{2})^2 + (\sqrt{2})^2)^{1/2} = 2$.

Sustituimos en (6.5) el divisor δ por $(1+i)\delta$ y tomando módulos,

$$|z| < |z_o|\frac{1}{\sqrt{2}}\left(1+\frac{1}{1+\sqrt{2}}\right) = |z_o|\frac{1}{\sqrt{2}}\frac{2+\sqrt{2}}{1+\sqrt{2}} = |z_o|.$$

Repitiendo este proceso mientras $|z_o|^2 > (1+\sqrt{2})|ab|$ llegaremos a una solución con $|z^2| \leq (1+\sqrt{2})|ab|$.

Queda por ver que z nunca puede ser 0, porque de ser así, la solución habría de ser necesariamente la trivial $(0,0,0)$. Si z fuera 0, es decir

$$z_o(aX^2+bY^2+cZ^2) - 2Z(ax_oX+by_oY+cz_oZ) = 0 \qquad (6.7)$$

Despejando, resulta que Z sólo podría valer

$$\begin{aligned} Z &= \frac{-2(ax_oX+by_oY) \pm \sqrt{4(ax_oX+by_oY)^2 + 4cz_o(az_oX^2+bz_oY^2)}}{2cz_o} \\ &= \frac{-(ax_oX+by_oY)}{cz_o} \pm \frac{\sqrt{ab(y_oX-x_oY)^2}}{cz_o} \end{aligned}$$

Pero no puede haber ningún entero Z obtenido así, ya que $\sqrt{ab(y_oX-x_oY)^2}$ es según los casos igual a $\sqrt{ab\frac{c^2}{2i}}$ o a $\sqrt{abc^2}$, y en ambos con valores irracionales por ser a, b, libres de cuadrados.

Esto completa la demostración.

Ejemplo **6.1** *Con ayuda del teorema 3.5 Hemos generado un ejemplo de ecuación que satisface la solución*

$$7-i,\ 2-5i,\ 1-2i$$

con los parametros $X = 1+i$, $Y = -i$, $Z = -1$. *La ecuación que resulta es:*

$$(-3+44i)\,x^2 + (59+30i)\,y^2 + (35+68i)\,z^2 = 0$$

Hemos parametrizado todas las soluciones de acuerdo con el teorema 3.3 y hemos hallado con $X = -2$, $Y = -1$ *otra más grande*

$$x_o = 111-97i, \quad y_o = 36+151i, \quad z_o = 73-60i$$

donde z_o satisface

$$|73-60i| = 94,4\cdots > \sqrt{(1+\sqrt{2})\,|-3+44i||59+30i|} = 83,9\ldots$$

Veamos que es posible encontrar una solución x, y, z en la que z satisfaga la cota del teorema. Debemos resolver la ecuación $y_oX - x_oY = c$.

Primero una solución de

$$(36+151i)\ -X(111-97i)\,Y = 1 \tag{6.8}$$

De la división en los racionales $\frac{x_o}{y_o} = \frac{111-97i}{36+151i} = -0.440\cdots - 0.842\cdots i$, de acuerdo con el teorema 5.7 hallo,

$$q_1 = -i \qquad r_1 = (111-97i) - (36+151i)(-i) = -61+40i$$

volviendo a dividir y_o por r_1 y repitiendo el proceso hasta que el resto sea 1 obtenemos,

$$\begin{aligned} q_2 &= 2 & r_2 &= -11-17i \\ q_3 &= 4i & r_3 &= 7-4i \\ q_4 &= 3i & r_4 &= 1+4i \\ q_5 &= 1+2i & r_5 &= 2i \\ q_6 &= -2 & r_6 &= 1 \\ q_7 &= -2i \end{aligned}$$

de acuerdo con la ecuación 2.4 tenemos todas las soluciones en paramétricas de la ecuación con:

$$\begin{aligned} \begin{bmatrix} X \\ Y \end{bmatrix} &= \begin{bmatrix} 1 & 0 \\ -i & 1 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 4i & 1 \end{bmatrix} \begin{bmatrix} 1 & 3i \\ 0 & 1 \end{bmatrix} \cdot \\ &\quad \cdot \begin{bmatrix} 1 & 0 \\ 1+2i & 1 \end{bmatrix} \begin{bmatrix} 1 & -2 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ -2i & 1 \end{bmatrix} \begin{bmatrix} T \\ 1 \end{bmatrix} = \\ &= \begin{bmatrix} 32+69i+(11-97i)T \\ 80+4i-(36+151i)T \end{bmatrix} \end{aligned}$$

Para $T = 0$ tenemos que una solución de $y_oX - x_oY = 1$ es $X = 32+69i$,

$Y = -(80 + 4i)$. *Luego una solución de* $y_oX - x_oY = c$ *es*

$$X = -3572 + 4591\,i, \quad Y = -2528 - 5580\,i$$

Al ser $N(c) = 5849$, *2 no divide a* $N(c)$ *y por tanto (1+1) no divide a c. Luego c no es múltiplo de* $(1 + i)$ *y estamos en el segundo caso en el que debemos buscar el valor de Z como el gaussiano más próximo a*

$$-\frac{ax_oX + by_oY}{cz_o} = 2378.3596\cdots + 2872.3208\cdots i$$

con la misma paridad que $[aX + bY + cZ]_{1+i} = [0]_{1+i}$. *Como*

$$[-cZ]_{1+i} = [aX + bY]_{1+i} = [-173040 - 576001\,i]_{1+i} = [1]_{1+i}$$

y como c no es múltiplo de $1 + i$ *necesariamente Z tiene la paridad de no ser múltiplo de* $1 + i$. *Siendo así, el gausiano multiplo de* $1 + i$ *más uno que es más próximo es* $Z = -2379 + 2872i$.

Estos tres valores de parámetros me generan a partir de las ecuaciones paramétricas la solución

$$x = 121 - 151i, \quad y = 47 + 151i, \quad z = -20 - 2i$$

en la cual

$$|z| < |z_o| \quad \text{y también} \quad |z| \leq \sqrt{(1 + \sqrt{2})|ab|}.$$

7

El teorema de Legendre en $\mathbb{Q}[t]$

$\mathbb{Q}[t]$, el anillo de los polinomios con indeterminada t sobre el cuerpo de los racionales es diferente a $\mathbb{Z}$ y $\mathbb{Z}[i]$ y otros dominios cuadráticos imaginarios similares. Es un anillo euclídeo con la norma,

$$|p| := \text{ el grado del polinomio}$$

(La norma del polinomio nulo no se define). Como tal, es posible en $\mathbb{Q}[t]$ la división euclídea, y para cualquier par p, q de polinomios, existen M, r polinomios tales que

$$p = Mq + r, \quad \text{con} \quad |r| < |q|.$$

Los dominios euclídeos son dominios de factorización única. En $\mathbb{Q}[t]$ las unidades son los racionales, y cualquier polinomio irreducible q, salvo factor por un racional es primo en $\mathbb{Q}[t]$.

En el sistema de clases residuales $\mathbb{Q}[t]_q$, para cierto polinomio q con grado $|q|$, las clases $[r]_q$ están representadas por polinomios de grado menor que $|q|$.

Definición 7.1 *Un polinomio f de $\mathbb{Q}[t]$ es resíduo cuadrático módulo q si existe un polinomio r tal que*

$$[r^2]_q = [f]_q \quad \textit{o equivalentemente} \quad \frac{r^2 - f}{q} \in \mathbb{Q}[t],$$

Siempre puede tomarse r, con $|r| < |q|$. Si f es resíduo cuadrático de q,

también lo es para cualquier múltiplo racional de q. Entonces q puede ser siempre representado por un polinomio en $\mathbb{Z}[t]$. Aunque f, g estén ambos en $\mathbb{Z}[t]$, r no necesariamente está en $\mathbb{Z}[t]$.

El sistema de clases residuales módulo un polinomio q de grado cero se reduce a un único elemento $Q[t]_q = \{[0]_q\}$ porque el resto en la división de un racional por un racional es siempre 0. Cualquier racional es entonces siempre resíduo cuadrático módulo cualquier polinomio de grado cero. Es decir que todas las ecuaciones con a, b, c raciones deberían ser resolubles cosa que no es cierto. El enunciado del teorema de Legendre en $\mathbb{Q}[t]$ debería considerar aparte del caso en que a, b, c sean los tres racionales, otros casos, porque la condición (iv) establecida en $\mathbb{Q}[t]$ sigue sin ser suficiente para que la ecuación de Legendre en $\mathbb{Q}[t]$ sea resoluble. Por ejemplo,

$$x^2 + y^2 - 3(t^2 + 1)z^2 = 0$$

satisface (iv) pero no es resoluble ya que de tener solución lo sería para cada t, en particular para $t_o = 0$ que implicaríia que $x + y^2 - 3z^2 = 0$ es una ecuación resoluble, lo que no es cierto porque -1 no es resíduo cuadrático de 3.

Previamente determinemos qué es una ecuación en su forma normal en $\mathbb{Q}[t]$.

Definición 7.2 *La ecuación $ax^2 + by^2 + cz^2 = 0$ en $\mathbb{Q}[t]$ está expresada en su forma normal si a, b, c son polinomios con coeficientes enteros, es decir $a, b, c \in \mathbb{Z}[t]$ y*

(ii) *a, b, c no contiene cuadrados,*

(iii) *a, b, c son primos dos a dos en $\mathbb{Z}[t]$.*

Cualquier ecuación puede expresarse en su forma normal. Primero eliminamos denominadores de los coeficientes y simplificamos obteniendo a, b, c con coeficientes enteros y (a, b, c)=1 en $\mathbb{Z}[t]$. Después eliminamos cuadrados, teniendo en cuenta que en general una ecuación $\alpha^2 ax^2 + \beta^2 by^2 + \gamma^2 cz^2$=0 tiene solución x, y, z si y sólo si $ax^2 + by^2 + cz^2$=0 tiene solución $\beta\gamma x, \alpha\gamma y, \beta\gamma z$. Por último, eliminamos los factores comunes por pares, siempre en $\mathbb{Z}[t]$, teniendo en cuenta que $pax^2 + pby^2 + cz^2$=0 tiene solución x, y, z si y sólo si $ax^2 + by^2 + pcz^2$=0 tiene solución px, py, z.

Como en el transcurso de la demostración del teorema necesitaremos aplicar una consecuencia del siguiente lema conocido como lema de Gauss.

Definición 7.3 *Sea P un polinomio en $\mathbb{Z}[t]$. Se llama contenido de P al máximo común divisor de los coeficientes de P.*

Si el contenido es 1 entonces el polinomio se dice **primitivo**. Cualquier polinomio P puede expresarse como

$$P = P_1 P_2$$

en donde P_1 es su contenido y P_2 es un polinomio primitivo de P, resultado de dividir P entre su contenido.

El lema de Gauss es importante en el análisis de la divisibilidad en $\mathbb{Z}[t]$:

Lema 7.1 (Lema de Gauss) *Sean*

$$P = P_1 P_2, \quad Q = Q_1 Q_2$$

polinomios en $\mathbb{Z}[t]$, con P_1, Q_1 contenidos y P_2, Q_2 polinomios primitivos respectivamente de P y Q. Entonces el contenido de PQ es $P_1 Q_1$.

Como consecuencia del lema, si $R \in \mathbb{Z}[t]$ divide a $S \in \mathbb{Z}[t]$ en $\mathbb{Q}[t]$, si S es en particular primitivo entonces siempre $\frac{R}{S} \in \mathbb{Z}[t]$.

El enunciado de la generalización del teorema de Legendre en $\mathbb{Q}[t]$ es el siguiente:

Teorema 7.1 *La ecuación*

$$ax^2 + by^2 + cz^2 = 0 \tag{7.1}$$

en el anillo de los polinomios $\mathbb{Q}[t]$, con a, b, c con coeficientes enteros, $abc \neq 0$, expresada en su forma normal en $\mathbb{Q}[t]$, es decir

(ii) *a, b, c libre de cuadrados,*

(iii) *a, b, c primos dos a dos en $\mathbb{Z}[t]$*

tiene solución no trivial de valores primos relativos dos a dos en $\mathbb{Q}[t]$ si y sólo si

(i) *$a^o x^2 + b^o y^2 + c^o z^2 = 0$ con a^o, b^o y c^o coeficientes de mayor grado de a, b y c respectivamente es resoluble en $\mathbb{Z}$,*

(iv) *$-bc$, $-ac$, $-ab$ son resíduos cuadrádricos de a, b y c respectivamente en $\mathbb{Q}[t]$.*

Probamos la necesidad de (i).

Si (x, y, z) es solución de (7.1), los tres polinomios ax^2, by^2 y cz^2 se cancelan sumando 0. Entonces:

En el caso en que el grado de uno de ellos, pongamos que ax, es estrictamente mayor que el de los otros dos, necesariamente $x = 0$ y deben cancelarse by^2 y cz^2:

Si $|by^2| = |cz^2|$, sus coeficientes de mayor grado deben a su vez cancelarse sumando $b^o y^2$ y $c^o z^2$ con lo que necesariamente $-b^o c^o = l^2$ es un cuadrado y entonces $(0, l, b^o)$ es solución de $a^o x^2 + b^o y^2 + c^o z^2 = 0$.

Si $|by^2| < |cz^2|$ la ecuación (7.1) no tiene otra solución que la trivial.

En el caso en que dos de ellos, digamos que ax^2 y by^2, tienen el mismo grado y el otro estrictamente menor, sus coeficientes de mayor grado deben cancelarse sumando $a^o x^2$ y $b^o y^2$ con lo que necesariamente $-a^o b^o = l^2$ es un cuadrado y entonces $(l, 0, a^o)$ es solución de $a^o x^2 + b^o y^2 + c^o z^2 = 0$.

En el caso en que los tres ax^2, by^2, cz^2, tienen el mismo grado, los coeficientes de mayor grado se cancelan sumando $a^o x^2$, $b^o y^2$ y $c^o z^2$, en consecuencia (x^o, y^o, x^o) es solución. Esto prueba la necesidad de (i).

La necesidad de (iv) ya se probó de manera general cualquiera que sea el dominio euclídeo en el lema 2.1.

Para hacer la demostración de la suficiencia, adaptamos la demostración por inducción que hace Dirichlet [6] (también Dickson [10] y Nagell [14]) del teorema de Legendre en $\mathbb{Z}$:

Podemos suponer que hemos reordenado la ecuación 7.1 de manera que los grados de los polinomios sean siempre $|a| \leq |b| \leq |c|$. Definimos el **Índice** I de la ecuación (7.1) al valor mediano $|ac|$ de la sucesión $|ab| \leq |ac| \leq |bc|$.

Probamos el toerema por inducción sobre el índice I. Primero que es cierto para I=0 y que, si es cierto para una ecuación de índice I', con $0 \leq I' < I$, entonces lo es para I.

El teorema es cierto para la ecuación de índice I=0. En este caso coincide con el teorema de Legendre en los enteros.

Supongamos que el índice es $I > 0$. Encontraremos otra ecuación

$$AX^2 + BY^2 + CZ^2 = 0$$

que satisfacerá igualmente las condiciones del teorema con índice menor y aplicaremos la hipótesis de inducción.

Como (7.1) satisface (iii), existe un polinomio R con $[R^2]_c$=$[-ab]_c$. Como

a es inversible en $\mathbb{Q}[t]_c$, sea r tal que

$$[(R/a)^2]_c = [r^2]_c = [-b/a]_c$$

que siempre podemos tomar de manera que $|r| < |c|$.

Multiplicamos por a, tenemos $[ar^2]_c = [-b]_c$, y existe entonces un polinomio M tal que,

$$ar^2 + b = cM. \tag{7.2}$$

Si M fuese 0, de $ar^2 = -b$, como a, b son libres de cuadrados tenemos $r^2 = 1$, entonces $a = -b$ y como a, b son primos dos a dos entonces a=1, b=-1 o al revés y $1, 1, 0$ es solución. Suponemos que $M \neq 0$.

Ni r ni M tienen necesariamente coeficientes enteros. Separamos $c = c_1c_2$, $c_1 \in \mathbb{Z}$, $c_2 \in \mathbb{Z}[t]$ primitivo con el máximo común divisor de los coeficientes de c_2 igual a 1. Sea $r = \dfrac{1}{h}r_1$ con h entero y r_1 polinomio con coeficientes enteros, $(r_1, h) = 1$. Escribo (7.2),

$$M = \frac{a\frac{r_1^2}{h^2} + b}{c_1c_2} = \frac{ar_1^2 + h^2b}{c_1c_2h^2} \tag{7.3}$$

como $ar_1^2 + h^2b \in \mathbb{Z}[t]$ y c_2 es primitivo, por el lema de Gauss anterior $\frac{ar_1^2+h^2b}{c_2} = M_1 \in \mathbb{Z}[t]$ entonces

$$\frac{c_2M_1}{c_1c_2h^2}, \quad c_2M_1 \in \mathbb{Z}[t] \tag{7.4}$$

y los tres términos de la igualdad

$$ar_1^2 + h^2b = c_2M_1 \tag{7.5}$$

están en $\mathbb{Z}[t]$.

Sea A el máximo común divisor A=(ar_1^2, h^2b, c_2M_1) de los tres términos que aparecen en la ecuación (7.5).

Si un divisor A_1 de A divide a b, no puede tener divisores comunes a a y c_2, por tanto A_1 divide necesariamente a r_1^2. Como A_1 no puede tener factores cuadrados por no tenerlos b, divide a r_1.

Si un divisor A_2 de A divide a a, no puede tener divisores comunes a b y c_2, por tanto A_2 divide necesariamente a a, y a h.

Podemos expresar A=A_1A_2, con (A_1, A_2)=1 y para ciertos α_1, α_2, β_1,

β_2 tenemos,

$$a = A_2\alpha_2, \quad r_1 = A_1\alpha_1 \quad h = A_2\beta_2, \quad b = A_1\beta_1 \quad c_2M_1 = c_2AC_1 \tag{7.6}$$

Como A divide en $\mathbb{Z}[t]$ a c_2M_1 entonces $c_2C_1 \in \mathbb{Z}[t]$. Como c_2 es polinomio primitivo, por el lema de Gauss $C_1 \in \mathbb{Z}[t]$. Sea k^2 el mayor cuadrado que divide a c_1C_1, definimos

$$B = \frac{ab}{A} = \alpha_2\beta_1, \quad C = \frac{c_1C_1}{k^2} \tag{7.7}$$

y consideramos la ecuación

$$AX^2 + BY^2 + CZ^2 = 0. \tag{7.8}$$

Es evidente que tal como están definidos, A, B, C son polinomios con coeficientes enteros.

Lema 7.2 *La ecuación* $AX^2 + BY^2 + CZ^2 = 0$ *satisface* (i)-(ii)-(iii)-(iv).

Como los divisores comunes de ar_1^2 y h^2b lo son de c_2M_1, A resulta ser el máximo común divisor de dos de los tres términos. Si sustituyo las igualdades de (7.6) en (7.5) y divido por A, obtengo

$$A_1\alpha_2\alpha_1^2 + A_2\beta_1\beta_2^2 = \frac{1}{c_1}c_2Ck^2 = c_2C_1 \tag{7.9}$$

donde los tres términos son primos dos a dos.

Como a, b son primos relativos y libre de cuadrados, $AB = ab$ implica que también A y B son primos relativos y libres de cuadrados. C es libre de cuadrados por definición.

Como los términos de (7.9) son primos dos a dos, C_1 es primo al producto de los dos primeros términos $A_1A_2\alpha_2\beta_1(\alpha_1\beta_2)^2 = AB(\alpha_1\beta_2)^2$ y como C_1 es primo con $\alpha_1\beta_2$ lo es con con AB. Por hipótesis c_1 no tiene divisores comunes con $ab = AB$ entonces también $c_1C_1 = Ck^2$ es primo con AB, C es primo con AB y por tanto con A y con B. Esto prueba (ii) y (iii).

Si f es un polinomio, sea

$$f^o := \text{coeficiente de mayor grado de} f$$

De las igualdades (7.6) y (7.7) obtengo

$$a^o = A_2\alpha_2^o, \quad b^o = A_1^o\beta_1^o, \quad c^o = c_1c_2^o \tag{7.10}$$

$$A^o = A_2A_1^o, \quad B^o = \frac{a^ob^o}{A^o} = \alpha_2^o\beta_1^o, \quad C^o = \frac{c_1C_1^o}{(k^o)^2} \tag{7.11}$$

Como $|a| \leq |b| \leq |c|$, en el caso en que $|b| < |c|$, como h es entero, entonces de la ecuación (7.5) podemos deducir que

$$(ar_1^o + h^2b)^o = (ar_1^2)^o = (c_2M_1)^o$$

y de la ecuación (7.9) tenemos,

$$A_1^o\alpha_2^o(\alpha_1^o)^2 = c_2^oC_1^o. \tag{7.12}$$

Si (x, y, z) es solución de $a^ox^2 + b^oy^2 + c^oz^2 = 0$ entonces tomando

$$X = \alpha_1^o\alpha_2^o\, x \quad Y = \alpha_1^oA_1^o\, y \quad Z = c_2^ok^o\, z$$

por (7.10), (7.11) y (7.12) tenemos que,

$$\begin{aligned} A^oX^2 + B^oY^2 + C^oZ^2 =& A^o(\alpha_1^o\alpha_2^o)^2x^2 + B^o(\alpha_1^oA_1^o)^2y^2 + C^o(c_1c_2^ok^o)^2z^2 \\ =& (A_1^o\alpha_2^o(\alpha_1^o)^2)(A_2\alpha_2^o)\, x^2 + (A_1^o\alpha_2^o(\alpha_1^o)^2)(A_1^o\beta_1^o)y^2 + \\ &+ (c_2^oC_1^o)(c_1c_2^o)\, z^2 \\ =& (c_2^oC_1^o)(a^ox^2 + b^oy^2 + c^ox^2) = 0 \end{aligned}$$

ya que $c_2^oC_1^o$ es distinto de 0. Entonces (X, Y, Z) es solución de

$$A^oX^2 + B^oY^2 + C^oZ^2 = 0.$$

Esto prueba (i) en este caso.

En el caso en que $|b| = |c|$, tenemos

$$(ar_1^o + h^2b)^o = (ar_1^2)^o + (h^2b)^o = (c_2M_1)^o$$

y de la ecuación (7.9) tenemos,

$$A_1^o\alpha_2^o(\alpha_1^o)^2 + A_2\beta_1^o\beta_2^2 = c_2^oC_1^o. \tag{7.13}$$

Si (x, y, z) es solución de $a^ox^2 + b^oy^2 + c^oz^2 = 0$ entonces tomando

$$X = \alpha_1^o\alpha_2^o\, x + \beta_1\beta_2^o\, y \quad Y = -A_2\beta_2^o\, x + \alpha_1^oA_1^o\, y \quad Z = (c_2^ok^o)\, z$$

por (7.10), (7.11) y (7.13) tenemos que,

$$\begin{aligned}A^oX^2+B^oY^2+C^oZ^2 =&(A_2^2B^o(\beta_2^o)^2+A^o(\alpha_1^o)^2(\alpha_2^o)^2)\,x^2+\\ &+(\beta_2^2A^o(\beta_1^o)^2+B^o(A_1^o)^2(\alpha_1^o)^2)\,y^2+(c_2^oC_1^o)(c_1c_2^o)\,z^2+\\ &+(2\beta_2A^o\alpha_1^o\alpha_2^o\beta_1^o-2\beta_2A_2A_1^oB^o\alpha_1^o)\,xy\\ =&(A_1^o\alpha_2^o(\alpha_1^o)^2+A_2\beta_1^o\beta_2^2)(a^ox^2+b^oy^2)+(c_2^oC_1^o)c^oz^2\\ =&(c_2^oC_1^o)(a^ox^2+b^oy^2+c^ox^2)=0\end{aligned}$$

luego (X,Y,Z) es solución de $A^oX^2+B^oY^2+C^oZ^2=0$. Esto completa la prueba de (i).

Multiplico en (7.9) por $A_1\alpha_2$,

$$(A_1\alpha_2\alpha_1)^2+A_1A_2\alpha_2\beta_1\beta_2^2=A_1\alpha_2c_2C_1,$$

y vemos que $-A_1A_2\alpha_2\beta_1\beta_2^2=-AB\beta_2^2$ es resíduo cuadrático de C_1 y como (β_2,C_1)=1, $-AB$ es resíduo cuadrático de C_1 y por tanto de $C=\frac{c_1}{k^2}C_1$.

Multiplico en (7.9) por c_2C,

$$(c_2Ck)^2-A_2\beta_1cC\beta_2^2=A_1\alpha_2cC\alpha_1^2$$

y vemos que:

$A_2\beta_1cC\beta_2^2$ y por tanto $A_2\beta_1cC$ son resíduos de A_1 y de α_2,
$A_1\alpha_2cC\alpha_1^2$ y por tanto $A_1\alpha_2cC$ son resíduos de A_2 y de β_1.

Además por hipótesis,

$-ac$ es resíduo de $b=A_1\beta_1$ y lo es de A_1 y de β_1
$-bc$ es resíduo de $a=A_2\alpha_2$ y lo es de A_2 y de α_2.

Entonces al ser ambos $A_2\beta_1cC$ y $-ac$ resíduos cuadráticos de A_1, también lo es el producto de los dos

$$-aA_2\beta_1Cc^2=-A_2\alpha_2A_2\beta_1Cc^2=-BCA_2^2c^2,$$

por tanto $-BC$ es resíduo cuadrático de A_1 y como A_2 es entero, lo es de $A=A_1A_2$.

Por último, como $-ac$ y $A_1\alpha_2cC$ son resíduos cuadráticos de β_1, lo es

el producto

$$-acA_1\alpha_2cC = -A_1A_2C(\alpha_2c)^2 = -AC(\alpha_2c)^2$$

y lo es $-AC$ de β_1. Sea u_1 con $[u_1^2]_{\beta_1} = [-AC]_{\beta_1}$.

Como $A_2\beta_1cC$ y $-bc$ son resíduos cuadráticos de α_2 lo es su producto

$$-bcA_2\beta_1cC = -A_1A_2C(\beta_1c)^2 = -AC(\beta_1c)^2$$

y lo es $-AC$ de α_2. Sea u_2 con $[u_2^2]_{\alpha_2} = [-AC]_{\alpha_2}$.

Por el teorema chino del resto, como $(\alpha_2, \beta_1) = 1$, existe una solución u común con $[u]_{\beta_1} = [u_1]_{\beta_1}$ y con $[u]_{\alpha_2} = [u_2]_{\alpha_2}$. Por tanto $u^2 + AC$ es divisible por β_1 y α_2 y por $\beta_1\alpha_2 = B$. Luego $-AC$ es resíduo cuadrático de B. Esto prueba (iv).

Veamos ahora que el índice de (7.8) es menor que I. Por una parte $|AB| \leq I$ ya que

$$|AB| = |ab| \leq |ac| = I.$$

Pero $|AC|$ es siempre menor que I: Despejamos $M = \frac{ar^2+b}{c}$ de (7.2), si $|b| < |c|$ entonces $|ar^2 + b| = |ar^2|$ ya que de lo contrario $M = 0$, y así, dado que $|r| < |c|$,

$$|AC| \leq |AC(\frac{k}{c_1h})^2| = |M| = \left|\frac{ar^2+b}{c}\right| = \left|\frac{ar^2}{c}\right| < \left|\frac{ac^2}{c}\right| = |ac| = I,$$

y si $|b| = |c|$, o bien $|ar^2 + b| = |ar^2|$, y como antes $|AC| < I$, o bien $|ar^2 + b| \leq |b|$ con lo que M sería un racional y el grado $|AC| = 0 < |ac| = I$.

Cualquiera que sea $|BC|$, en todos los casos a continuación vemos que el índice de la ecuación (7.8) es menor o igual que I. Cuando es igual, una misma nueva reducción sobre (7.8), nos dará otra de índice siempre menor:

Caso 1. $|a| < |b| < |c|$. Tenemos $|ab| < |ac| < |bc|$. Tanto $|AC|$ como $|AB|$ son menores que I. Cualquiera que sea el valor de $|BC|$, el índice de (7.8) es $< I$.

Caso 2. $|a| = |b| < |c|$. Tenemos $|ab| < |ac| = |bc|$. La ecuación (7.8) también, como en el caso 1, satisface $|AB| = |ab| < |ac| = I$, $|AC| < |ac| = I$ y tiene índice menor que I.

Caso 3. $|a| < |b| = |c|$. En este caso, $|ab| = |ac| < |bc|$. Tenemos $|AB| = |ab| = I$ y $|AC| < |ac| = I$. Si $|BC|$ fuera menor que I se habría obtenido la ecuación reducida. Si $|BC|$ fuera mayor que I entonces la ecuación obtenida

tendría indice también I pero con $|AC| < |AB| < |BC|$ y estaríamos en el caso 1 y volveríamos a aplicar el mismo proceso a esta última ecuación hasta obtener otra de indice más reducido. Si $|BC| = I$ la ecuación obtenida también tiene índice I pero como $|AC| < |AB| = |BC|$ estaríamos con una ecuación como en el caso 2 a la que volviéndole a aplicar el proceso llegaríamos a otra de índice menor.

Caso 4. $|a| = |b| = |c|$. Tenemos $|ab| = |ac| = |bc|$. $|AB| = |ab| = I$ y también $|AC| < |ac| = I$ y como en el caso anterior cualquiera que fuera $|BC|$, el índice sería menor que I, o igual a I en una nueva ecuación que está en el caso 2.

Supongamos que la ecuación reducida (7.8) tiene índice $< I$. Aplicamos la hipótesis de inducción y sea (X, Y, Z) una solución no trivial. Mediante la transformación

$$x = c_1(A_1\alpha_1 X - \beta_1\beta_2 Y), \qquad y = c_1(A_2\beta_2 X + \alpha_1\alpha_2 Y), \qquad z = CkZ \tag{7.14}$$

se tiene que,

$$\begin{aligned} ax^2 + by^2 + cz^2 =& c_1^2\left(b\beta_2^2A_2^2 + a\alpha_1^2A_1^2\right)X^2 \\ &+ c_1^2\left(2\alpha_1\alpha_2 b\beta_2 A_2 - 2a\alpha_1\beta_1\beta_2 A_1\right)XY + \\ &+ c_1^2\left(a\beta_1^2\beta_2^2 + \alpha_1^2\alpha_2^2 b\right)Y^2 + ck^2C^2Z^2, \end{aligned}$$

y por (7.6), (7.7) y (7.9) resulta

$$\begin{aligned} &= c_1^2(A_2\beta_1\beta_2^2 + A_1\alpha_2\alpha_1^2)A_1A_2X^2 + c_1^2(A_2\beta_1\beta_2^2 + A_1\alpha_2\alpha_1^2)\alpha_2\beta_1Y^2 + cCk^2CZ^2 \\ &= c_1^2c_2C_1(AX^2 + BY^2) + cCk^2(CZ^2) = c_1^2c_2C_1(AX^2 + BY^2 + CZ^2) = 0, \end{aligned}$$

y como $c_1^2c_2C_1 \neq 0$, (x, y, z) es solución de (7.1).

Si la ecuación (7.8) tiene índice $= I$, una nueva misma redución nos garantiza una ecuación $A'X'^2 + B'Y'^2 + C'Z'^2 = 0$ de índice $< I$ que por hipótesis tiene solución (X', Y', Z'), con lo que (7.8) tendrá solución

$$X = c_1'(A_1'\alpha_1'X' - \beta_1'\beta_2'Y'), \qquad X = c_1'(A_2'\beta_2'X' + \alpha_1'\alpha_2'Y'), \qquad Z = C'k'Z'$$

y (7.1) tendrá a (x, y, z) de (7.14).

Sólo queda comprobar que la solución obtenida mediante esa transformación (7.14) no es la trivial. Si lo fuera, x=y=z=0, la eliminación de X de (7.14), nos da $(A_1\alpha_2\alpha_1^2 + A_2\beta_1\beta_2^2)Y = 0$. El primer factor no es cero por (7.9), por tanto $Y = 0$, y también lo serían X=0, y Z=0 lo que es falso.

Esto completa la demostración del teorema.

La existencia de soluciones minimales de la ecuación en $\mathbb{Q}[t]$ que generalizará el teorema de Holzer como se ha hecho en [29] con los enteros de Gauss también será posible y lo desarrollamos en el próximo capítulo.

8

El teorema de Holzer en $\mathbb{Q}[t]$

Las cotas de Holzer varían dependiendo de la norma definida. En este caso, las cotas afectan al grado de los coeficientes. En el anterior capítulo probamos el teorema de Legendre en $\mathbb{Q}[t]$,

Teorema. *La ecuación $ax^2 + by^2 + cz^2 = 0$ en $\mathbb{Q}[t]$ con a, b, c polinomios con coeficientes enteros, $abc \neq 0$, expresada en su forma normal en $\mathbb{Q}[t]$, tiene soluciones no triviales en $\mathbb{Q}[t]$ if y sólo si,*

(i) *$a^o x^2 + b^o y^2 + c^o z^2 = 0$ ecucación con los coeficientes de mayor grado de a, b, c es resoluble en $\mathbb{Z}$,*

(iv) *$-bc$, $-ac$, $-ab$ son resíduos cuadrádricos de a, b y c respectivamente en $\mathbb{Z}$ si a, b, c son enteros. Si a, b, c no son los tres enteros, $-bc$, $-ac$, $-ab$ son resíduos cuadrádricos de a, b y c en $\mathbb{Q}[t]$.*

De la necesidad de (i) se deduce que a^o, b^o, c^o no pueden tener todos el mismo signo. Al menos dos de los coeficientes de mayor grado son del mismo signo, podemos reordenar y cambiar el signo a la ecuación si es necesario, y suponer siempre que los coeficientes de mayor grado son de signo positivo en a y b y de signo negativo en c.

Definición 8.1 *La ecuación resoluble $ax^2 + by^2 + cz^2 = 0$ en $\mathbb{Q}[t]$, expresada en su forma normal, está expresada en* **forma normal reordenada** *si además,*

(v) *Los coeficientes de mayor grado de a, b son positivos y el coeficiente de mayor grado de c es negativo*

En $\mathbb{Z}$, el cociente M de la división euclídea $p = qM + r$, $|r| \leq \frac{1}{2}$ ($|r|$ es el valor absoluto de r), entre p, q enteros, es el entero más próximo a $\frac{p}{q}$. La idea de polinomio más próximo en $\mathbb{Q}[t]$ es similar a la de $\mathbb{Z}$,

Definición 8.2 *Sean p, q polinomios de $\mathbb{Q}[t]$, $|p| > |q|$. Si*

$$p = Mq + r, \quad con \quad |r| < |q|$$

se dice que M es el **polinomio más próximo** *a $\frac{p}{q}$.*

El siguiente lema expone algunas propiedades sobre el grado que usaré, cuya demostración es evidente.

Lema 8.1 *Sean p, q, r, r polinomios en $\mathbb{Q}[t]$*

a) $|pq| = |p| + |q|, \quad |p^n| = n|p| \quad n > 0, n \in \mathbb{Z}$.

b) $\max\{|p|, |q|\} \geq |p + q|$.

c) *Si $\frac{p}{q} = \frac{r}{s}$, entonces $|p| - |q| = |r| - |s|$.*

Adapto de nuevo la demostración de Mordell [18] del teorema de Holzer en los enteros para probar que el teorema que sigue con cotas en los grados de los coeficientes en $\mathbb{Q}[t]$ es cierto:

Teorema 8.1 *La ecuación*

$$ax^2 + by^2 + cz^2 = 0 \tag{8.1}$$

con coeficientes a, b, c en los polinomios racionales $\mathbb{Q}[t]$, expresada en su forma normal en $\mathbb{Q}[t]$, si tiene una solución en $\mathbb{Q}[t]$, entonces tiene una solución (x, y, z) en donde

$$|x| \leq \frac{1}{2}(|b| + |c|), \quad |y| \leq \frac{1}{2}(|a| + |c|), \quad |z| \leq \frac{1}{2}(|a| + |b|) \tag{8.2}$$

Si la ecuación está expresada en su forma normal reordenada en $\mathbb{Q}[t]$, si $|ab|$ es impar entonces las tres desigualdades son estrictas.

La demostración consistirá en probar que si existe una solución en $\mathbb{Q}[t]$

$$(x_o, y_o, z_o) \tag{8.3}$$

que suponemos primitiva, es decir sin divisores comunes salvo unidades, tal que

$$|z_o| > \frac{1}{2}(|a| + |b|),$$

entonces se puede encontrar a partir de ella otra (x, y, z) con $|z| < |z_o|$.

Previamente para nuestro propósito, el lema que sigue nos asegura la existencia de inverso de y_o en $\mathbb{Q}[t]_c$ y la reslubilidad de la ecuación $y_oX - x_oY = c$.

Lema 8.2 *Si x_o, y_o, z_o es solución primitiva de ecuación* (8.1)*, entonces $(x_o, y_o) = (y_o, c) = 1$ en $\mathbb{Q}[t]$.*

Si $(x_o, y_o) \neq 1$, tendríamos $x_o = px'$, $y_o = py'$ con p primo común, con $-cz_o^2 = a(px')^2 + b(py')^2$, tomando clases residuales módulo p^2,

$$[-cz_o^2]_{p^2} = [p^2]_{p^2}[ax'^2 + by'^2]_{p^2} = [0]_{p^2}$$

lo que no es posible ya que p no divide a z_o y p^2 no o hace a z_o^2, y tampoco p^2 divide a c que está libre de cuadrados.

Si $(y_o, c) \neq 1$, existiría un p divisor común de c y de y_o, como $ax_o^2 = -by_o^2 - cz_o^2$ y como p no divide a a, debe hacerlo a x_o^2 y en consecuencia a x_o lo que es una contradicción porque $(x_o, y_o) = 1$.

El lema está probado.

Parametrizo las soluciones de la ecuación a partir de una solución conocida (x_o, y_o, z_o) con las fórmulas de Réalis [7] válidas en cualquier dominio euclídeo.

En particular en $\mathbb{Q}[t]$, éstas fórmulas se obtienen imponiendo que

$$(x_o + tX, y_o + tY, z_o + tZ) \tag{8.4}$$

sea una solución en el cuerpo $\mathbb{Q}(t)$ de fracciones de los polinomios racionales, con X, Y, Z parámetros $\in \mathbb{Q}[t]$, $t \in \mathbb{Q}(t)$, $t \neq 0$. Sustituimos en (8.1) y obtengo

$$\begin{aligned} 0 = a(x_o + tX)^2 + b(y_o + tY)^2 + c(z_o + tZ)^2 = \\ ax_o^2 + by_o^2 + cz_o^2 + (aX^2 + bY^2 + cZ^2)t^2 + 2t(ax_oX + by_oY + cz_oZ) = \\ t((aX^2 + bY^2 + cZ^2)t + 2(ax_oX + by_oY + cz_oZ)). \end{aligned}$$

Como $t \neq 0$, obtengo $t = \frac{-2(ax_oX + by_oY + cz_oZ)}{aX^2 + bY^2 + cZ^2}$ que sustituido en (8.4) nos da una parametrización de las soluciones en $\mathbb{Q}(t)$ de (8.1), multiplicando por $aX^2 + bY^2 + cZ^2$ obtengo soluciones en $\mathbb{Q}[t]$,

$$\begin{aligned} x_o(aX^2 + bY^2 + cZ^2) - 2X(ax_oX + by_oY + cz_oZ) \\ y_o(aX^2 + bY^2 + cZ^2) - 2Y(ax_oX + by_oY + cz_oZ) \\ z_o(aX^2 + bY^2 + cZ^2) - 2Z(ax_oX + by_oY + cz_oZ) \end{aligned} \tag{8.5}$$

Estas soluciones no son necesariamente primitivas y pueden tener un divisor común.

Lema 8.3 *Si X, Y son polinomios tales que*

$$Xy_o - Yx_o = c,$$

entonces c entonces divide a las tres expresiones de (8.5).

Si $Xy_o - Yx_o = c$, tomando clases residuales tenemos $[Xy_o - Yx_o]_c = [0]_c$, y como $(c, y_o) = 1$, y_o es inversible en $\mathbb{Q}[t]_c$ y podemos despejar

$$[X]_c = [Yx_o/y_o]_c,$$

y sustituir en $[aX^2 + bY^2 + cZ^2]_c$,

$$\begin{aligned}[a(Yx_o/y_o)^2 + bY^2 + cZ^2]_c &= \left[(ax_o^2Y^2 + by_o^2Y^2 + cy_o^2Z^2)/y_o^2)\right]_c = \\ &= \left[(-cz_o^2Y^2 + cy_o^2Z^2)/y_o^2\right]_c = \left[c(-z_o^2Y^2 + y_o^2Z^2)/y_o^2\right]_c = [0]_c\end{aligned}$$

y en $[ax_oX + by_oY + cz_oZ]_c$,

$$\begin{aligned}[(ax_o(Yx_o/y_o) + by_oY + cz_oZ]_c &= \left[(ax_o^2Y + by_o^2Y + cy_o^2Z)/y_o)\right]_c = \\ &= \left[(-cz_o^2Y + cy_o^2Z)/y_o\right]_c = \left[c(-z_o^2Y + y_o^2Z)/y_o\right]_c = [0]_c,\end{aligned}$$

y obtenemos múltiplos de c. Por tanto las expresiones de (8.5) también son múltiplos de c lo que prueba el lema.

Considero entonces la solución (x, y, z) dada por,

$$\begin{aligned}x &= \frac{1}{c}(x_o(aX^2 + bY^2 + cZ^2) - 2X(ax_oX + by_oY + cz_oZ)) \\ y &= \frac{1}{c}(y_o(aX^2 + bY^2 + cZ^2) - 2Y(ax_oX + by_oY + cz_oZ)) \\ z &= \frac{1}{c}(z_o(aX^2 + bY^2 + cZ^2) - 2Z(ax_oX + by_oY + cz_oZ))\end{aligned} \tag{8.6}$$

con X, Y solución cualquiera de $Xy_o - Yx_o = c$, y con el valor de Z que determinaré después.

Manipulamos la ecuación (8.6) para poder comparar z con z_o:

$$\begin{aligned}
\frac{-z}{z_o} &= \frac{2Z(ax_oX + by_oY + cz_oZ)}{cz_o} - \frac{z_o(aX^2 + bY^2 + cZ^2)}{cz_o} \\
&= Z^2 + 2Z(\frac{ax_oX + by_oY}{cz_o}) - \frac{aX^2 + bY^2}{c} \\
&= (Z + \frac{ax_oX + by_oY}{cz_o})^2 - (\frac{ax_oX + by_oY}{cz_o})^2 - \frac{aX^2 + bY^2}{c} \\
&= \frac{(ax_oX + by_oY + cz_oZ)^2}{c^2z_o^2} - \frac{(ax_oX + by_oY)^2}{c^2z_o^2} - \frac{cz_o^2(aX^2 + bY^2)}{c^2z_o^2} \\
&= \frac{(ax_oX + by_oY + cz_oZ)^2 - (ax_oX + by_oY)^2 - cz_o^2(aX^2 + bY^2)}{c^2z_o^2} \qquad (8.7) \\
&= \frac{(ax_oX + by_oY + cz_oZ)^2}{c^2z_o^2} \\
&\quad - \frac{1}{c^2z_o^2}(aX^2cz_o^2 + bY^2cz_o^2 + a^2x_o^2X^2 + b^2y_o^2Y^2 + 2abx_oy_oXY)
\end{aligned}$$

como $cz_o^2 = -ax_o^2 - by_o^2$,

$$\begin{aligned}
&= \frac{(ax_oX + by_oY + cz_o)^2 + ab(y_o^2X^2 - 2x_oy_oXY + x_o^2Y^2)}{c^2c_o^2} \\
&= \frac{(ax_oX + by_oY + cz_oZ)^2 + ab(y_oX - x_oY)^2}{c^2z_o^2} \qquad (8.8)
\end{aligned}$$

y siendo $y_oX - x_oY = c$ tenemos que

$$\frac{-z}{z_o} = \frac{(ax_oX + by_oY + cz_oZ)^2 + c^2ab}{c^2z_o^2} \qquad (8.9)$$

La elección de Z se hace de acuerdo al lema,

Lema 8.4 *Si $z_o > \frac{1}{2}(|a| + |b|)$ y Z es el polinomio más próximo a*

$$\frac{ax_oX + by_oY}{-cz_o}$$

entonces $|z| < |z_o|$.

Si Z es el polinomio cociente de dividir $ax_oX + by_oY$ entre $-cz_o$, el resto de esa división es $ax_oX + by_oY + cz_oZ$. Este resto tiene grado menor que el

de $-cz_o$, luego

$$|(ax_oX + by_oY + cz_oZ)^2| < |c^2z_o^2| \tag{8.10}$$

y también, si por hipótesis $|ab| < |z_o^2|$ se tiene

$$|c^2ab| < |c^2z_o^2|. \tag{8.11}$$

Luego por (8.9), (8.10) y (8.11) y el lema (8.1) se tiene

$$\begin{aligned} |z_o| - |z| =& |c^2z_o| - |(ax_oX + by_oY + cz_oZ)^2 + c^2ab| \geq \\ \geq& |c^2z_o| - \max\{\, |(ax_oX + by_oY + cz_oZ)^2|,\, |c^2ab| \,\} \geq \\ \geq& 1, \end{aligned}$$

cualquiera que fuera el máximo. Por tanto $|z| < |z_o|$.

Si z fuera el poliniomio 0, como los coeficientes de mayor grado de a y b son positivos, $ax_o^2 + by_o^2 + cz_o^2 = 0$ es sólo posible si $y_o = 0$, y $z_o = 0$ y la solución necesariamente sería la trivial $(0, 0, 0)$.

El siguiente lema prueba que $z \neq 0$.

Lema 8.5 *El polinomio z anterior es siempre distinto de 0.*

Si z fuera el polinomio 0, también lo serían x, y. Entonces de las ecuaciones (8.6) tenemos

$$x_o(aX^2 + bY^2 + cZ^2) = 2X(ax_oX + by_oY + cz_oZ) \tag{8.12}$$

$$y_o(aX^2 + bY^2 + cZ^2) = 2Y(ax_oX + by_oY + cz_oZ) \tag{8.13}$$

$$z_o(aX^2 + bY^2 + cZ^2) = 2Z(ax_oX + by_oY + cz_oZ). \tag{8.14}$$

Multiplicando las anteriores expresiones respectivamente por ax_o, by_o, cz_o respectivamente y sumando las ecuaciones que resultan, tenemos

$$(ax_o^2 + by_o^2 + cz_o^2)(aX^2 + bY^2 + cZ^2) = 2(ax_oX + by_oY + cz_oZ)^2$$

que implica

$$ax_oX + by_oY + cz_oZ = 0. \tag{8.15}$$

Entonces de las ecuaciones (8.12), (8.13) tenemos

$$x_o(aX^2 + bY^2 + cZ^2) = y_o(aX^2 + bY^2 + cZ^2) = 0,$$

y como $(x_o, y_o) = 1$ necesariamente

$$aX^2 + bY^2 + cZ^2 = 0. \tag{8.16}$$

De los numeradores de (8.7) y (8.8), y por (8.15) y (8.16) obtengo

$$\begin{aligned} ab(y_oY - x_oY)^2 &= -(ax_oX + by_oY)^2 - cz_o^2(aX^2 + bY^2) \\ &= -(-cz_oZ)^2 - cz_o^2(-cZ^2) = 0, \end{aligned}$$

que contradice $y_oX - x_oY = c \neq 0$. Luego $z \neq 0$ y el lema está probado.

Repetimos este proceso con la solución obtenida (x, y, z) que pasa a ser ahora la solución (x_o, y_o, z_o) de (8.3) y mientras sea $|z_o^2| = 2|z_o| > |ab| = |a| + |b|$ y hasta que obtengamos una solución con z con desigualdad no necesariamente estricta,

$$|z^2| = 2|z| \leq |ab| = |a| + |b|,$$

es decir

$$|z| \leq \frac{1}{2}(|a| + |b|).$$

Las otras dos desigualdades se cumplen simultáneamente cuando se ha hecho la reducción de z sobre la ecuación en su forma normal reordenada. Como los coeficientes de mayor grado en a y b son positivos y en c negativo, entonces se cumple siempre que

$$|ax^2| \leq |ax^2 + by^2| = | - cz^2| \tag{8.17}$$

$$|by^2| \leq |ax^2 + by^2| = | - cz^2|, \tag{8.18}$$

y si (x, y, z) es solución con $|z| \leq \frac{1}{2}(|a| + |b|)$, entonces por (8.17)

$$|a| + 2|x| \leq |c| + 2|z| \leq |c| + |a| + |b|,$$

despejando $|x|$

$$|x| \leq \frac{1}{2}(|b| + |c|).$$

Igual para $|y|$ con (8.18) y se tiene que

$$|y| \leq \frac{1}{2}(|a| + |c|).$$

Por último, Si $|z| \leq \frac{1}{2}(|a| + |b|)$ y $|ab|$ es impar entonces necesariamente

$|z| < \frac{1}{2}(|a| + |b|)$ y las otras dos desigualdades estrictas se obtienen como antes.

9

Soluciones enteras de la ecuación de legendre en $\mathbb{Q}[t]$

No siempre una ecuación resoluble en $\mathbb{Q}[t]$ tiene soluciones enteras, pero si la tiene es única salvo múltiplos o cambio de sus signos. El teorema es:

Teorema 9.1 *La ecuación*

$$ax^2 + by^2 + cz^2 = 0 \tag{9.1}$$

en $\mathbb{Q}[t]$, expresada en su forma normal, reordenada de manera que los grados de los coeficientes son $|a| \leq |b| \leq |c|$, tiene solución entera (x_o, y_o, z_o) única salvo múltiplos, si y solo si $(y_o/x_o)^2$ y $(z_o/x_o)^2$ son representantes racionales de las clases,

$$[-a/b]_c = [(y_o/x_o)^2]_c, \qquad [-a/c]_b = [(z_o/x_o)^2]_b. \tag{9.2}$$

Supongamos que (x_o, y_o, z_o) es solución entera, entonces

$$[ax_o^2 + by_o^2]_c = [0]_c, \tag{9.3}$$

multiplicando (9.3) por $[1/by_o^2]_c$,

$$[((x_o^2/y_o^2)(a/b) + 1)]_c = [0]_c. \tag{9.4}$$

Como $[a/b]_c \neq [0]_c$, despejamos $[-a/b]_c$ y tenemos,

$$[-a/b]_c = [(y_o/x_o)^2]_c. \tag{9.5}$$

De la misma forma se obtiene que

$$[-a/c]_b = [(z_o/x_o)^2]_b, \tag{9.6}$$

lo que prueba la condición necesaria del teorema.

Supongamos que (9.2) es cierto, entonces $[-a]_c = [(by_o/x_o)^2]_c$ es decir, existe un polinomio M tal que

$$a + b(y_o/x_o)^2 = cM. \tag{9.7}$$

Como $|a| \leq |b| \leq |c|$, y y_o/x_o es racional entonces

$$|a + b(y_o/x_o)^2| \leq |c| \tag{9.8}$$

con lo que

$$|M| = |\frac{a + b(y_o/x_o)^2}{c}|$$

sólo puede ser 0 si el grado en (9.8) es estrictamente menor, o un racional si es igual.

En el primer caso si $M = 0$, entonces $ax_o^2 + by_o^2 = 0$, lo que es sólo posible, puesto que $-ab$ es libre de cuadrados y primos dos a dos en $\mathbb{Z}[t]$, si $-ab = 1$ y entonces $(x_o, y_o, 0) = (1, 1, 0)$ es solución de (9.1).

En el segundo caso si M es racional, tomando clases residuales módulo b tenemos,

$$[a]_b = [a + b(y_o/x_o)^2]_b = [cM]_b, \tag{9.9}$$

de donde podemos despejar

$$[-a/c]_b = [-M]_b. \tag{9.10}$$

Pero como M es racional, necesariamente $M = -(z_o/x_o)^2$.

Por tanto por la ecuación (9.7) tenemos

$$a \cdot 1^2 + b(y_o/x_o)^2 = -c(z_o/x_o)^2 \tag{9.11}$$

es decir, que (x_o, y_o, z_o) es solución de la ecuación (9.1).

Si (x_1, y_1, z_1) es cualquier otra solución entera de (9.1) se tiene

$$ax_1^2 + by_1^2 + cz_1^2 = 0 \tag{9.12}$$

y entonces

$$[-a/b]_c = [(y_1/x_1)^2]_c \qquad [-a/c]_b = [(z_1/x_1)^2]_b \tag{9.13}$$

con lo que necesariamente (x_1, y_1, z_1) es múltiplo de (x_o, y_o, z_o) aunque quizá con otros signos. La condición es suficiente lo que prueba el teorema.

El teorema resuelve el problema de encontrar las soluciones enteras de un sistema,

Teorema 9.2 *El sistema de ecuaciones en* $\mathbb{Z}$*,*

$$\begin{aligned} a_o x^2 + b_o y^2 + c_o z^2 &= 0 \\ a_1 x^2 + b_1 y^2 + c_1 z^2 &= 0 \\ &\cdots \\ a_n x^2 + b_n y^2 + c_n z^2 &= 0 \end{aligned}$$

con $a = a_o + a_1 t \cdots + a_n t^n$*,* $b = b_o + b_1 t \cdots + b_n t^n$*,* $c = c_o + c_1 t \cdots + c_n t^n$ *primos dos a dos y libres de cuadrados en* $\mathbb{Z}[t]$*, tiene una única solución entera* (x_o, y_o, z_o)*, salvo múltiplos, si y sólo si*

$$\left[-\frac{(a_o + a_1 t + \cdots + a_n t^n)}{(b_o + b_1 t + \cdots + b_n t^n)}\right]_{c_o + c_1 t + \cdots + c_n t^n} = [(y_o/x_o^2]_{c_o + c_1 t + \cdots + c_n t^n} \tag{9.14}$$

$$\left[-\frac{(a_o + a_1 t + \cdots + a_n t^n)}{(c_o + c_1 t + \cdots + c_n t^n)}\right]_{b_o + b_1 t + \cdots + b_n t^n} = [(z_o/x_o)^2]_{b_o + b_1 t + \cdots + b_n t^n} \tag{9.15}$$

9.1 Ecuaciones de grados hasta 1

Las ecuaciones resolubles con coeficientes de grados hasta 1 admiten fórmula. Ello se debe a que los representantes de clases residuales de polinomios de grado 1 son siempre racionales, en particular, un residuo cuadrático de un polinomio de grado 1 es siempre el cuadrado de un racional.

La ecuación

$$a_o x^2 + b_o y^2 + (c_o + c_1 t) z^2 = 0$$

es trivial ya que si tenemos que $-a_a b_o$ es residuo cuadrático de $c_o + c_1 t$, es decir $-a_o b_o = k^2$ es un cuadrado con k racional, como a y b son libres de

cuadrados necesariamente $-a_o b_o = 1^2 = 1$, $a_o = -b_o = 1$ y la ecuación tiene solución $(1, 1, 0)$.

Consideremos pues la ecuación

$$(a_o + a_1 t)x^2 + (b_o + b_1 t)y^2 + (c_o + c_1 t)z^2 = 0, \tag{9.16}$$

con $b_1, c_1 \neq 0$.

Las clases de a, b módulo c

$$[a]_c = [\frac{a_1 c_o - a_o c_1}{c_1}]_c, \quad [b]_c = [\frac{b_1 c_o - b_o c_1}{c_1}]_c, \tag{9.17}$$

y del inverso de b módulo c

$$[1/b]_c = [\frac{c_1}{b_1 c_o - b_o c_1}]_c \tag{9.18}$$

están representados respectivamente por racionales, entonces

$$[-a/b]_c = [-a]_c[1/b]_c = \left[\frac{-(a_1 c_o - a_o c_1)}{b_1 c_o - b_o c_1}\right]_c. \tag{9.19}$$

De igual manera obtenemos

$$[-a/c]_b = [-a]_b[1/c]_b = \left[\frac{-(a_1 b_o - a_o b_1)}{c_1 b_o - c_o b_1}\right]_b. \tag{9.20}$$

De acuerdo entonces con el teorema, (9.26) tiene solución entera (x_o, y_o, z_o) si y sólo si

$$\frac{a_1 c_o - a_o c_1}{c_1 b_o - c_o b_1} = (y_o/x_o)^2 \quad \text{y} \quad \frac{b_1 a_o - b_o a_1}{c_1 b_o - c_o b_1} = (z_o/x_o)^2 \tag{9.21}$$

son cuadrados.

Pero esto cocurrirá siempre si la ecuación es resoluble. La ecuación satisface la condición (iv) del teorema de Legendre, y existen dos polinomios de grado cero, es decir dos racionales R_c, R_b con

$$[R_c^2]_c = [-ab]_c, \qquad [R_b^2]_b = [-ac]_b. \tag{9.22}$$

El cálculo de los restos $[-ab]_c$, $[-ac]_b$ da,

$$[-(a_o+a_1t)(b_o+b_1t)]_c=[\frac{(a_1c_o-a_oc_1)(c_1b_o-c_ob_1)}{c_1^2}]_c=[R_c^2]_c$$
$$[-(a_o+a_1t)(c_o+c_1t)]_b=[\frac{(b_1a_o-b_oa_1)(c_1b_o-c_ob_1)}{b_1^2}]_b=[R_b^2]_b$$

por lo que necesariamente serán cuadrados

$$\begin{aligned}(a_1c_o-a_oc_1)(c_1b_o-c_ob_1)&=(c_1R_c)^2\\(b_1a_o-b_oa_1)(c_1b_o-c_ob_1)&=(b_1R_b)^2,\end{aligned}\tag{9.23}$$

y entonces

$$\frac{a_1c_o-a_oc_1}{c_1b_o-c_ob_1}=(\frac{c_1R_c}{c_1b_o-c_ob_1})^2\tag{9.24}$$
$$\frac{b_1a_o-b_oa_1}{c_1b_o-c_ob_1}=(\frac{b_1R_b}{c_1b_o-c_ob_1})^2\tag{9.25}$$

son cuadrados. Hemos probado

Teorema 9.3 *La ecuación expresada en su forma normal,*

$$(a_o+a_1t)x^2+(b_o+b_1t)y^2+(c_o+c_1t)z^2=0,\tag{9.26}$$

si tiene soluciones, tiene la solución entera

$$(c_1b_o-c_ob_1,\,c_1R_c,\,b_1R_b)\tag{9.27}$$

única salvo múltiplos.

también podemos resumir,

Teorema 9.4 *La ecuación*

$$(a_o+a_1t)x^2+(b_o+b_1t)y^2+(c_o+c_1t)z^2=0$$

expresada en su forma normal, con $c_1\neq 0$, tiene solución si y sólo si

$$\frac{a_1c_o-a_oc_1}{c_1b_o-c_ob_1},\quad\frac{b_1a_o-b_oa_1}{c_1b_o-c_ob_1},$$

son cuadrados en $\mathbb{Q}$*. En ese caso una solución en* $\mathbb{Q}$ *es*

$$x = 1, \quad y = \sqrt{\frac{a_1c_o - a_oc_1}{c_1b_o - c_ob_1}}, \quad z = \sqrt{\frac{b_1a_o - b_oa_1}{c_1b_o - c_ob_1}}$$

y la obtenida en $\mathbb{Z}$ *tras eliminar denominadores es la única salvo múltiplos.*

Por ejemplo, la ecuación

$$(13 + 67t)x^2 - (57 + 72t)y^2 + (20 - 19t)z^2 = 0,$$

es resoluble dado que

$$\frac{a_1c_o - a_oc_1}{c_1b_o - c_ob_1} = (\frac{23}{29})^2, \qquad \frac{b_1a_o - b_oa_1}{c_1b_o - c_ob_1} = (\frac{31}{29})^2$$

y la única solución entera es 29, 23, 31.

10

Conclusiones

He investigado y desarrollado en este trabajo lo que se sabía acerca de la ecuación de Legendre. Hemos podido comprobar que eran posibles generalizaciones. Se ha demostrado,

1. La generalización del teorema de Legendre en $\mathbb{Q}[t]$.

2. La generalización del teorema de Holzer en $\mathbb{Z}[i]$.

3. La generalización del teorema de Holzer en $\mathbb{Q}[t]$

4. Las condiciones necesarias y suficientes para que una ecuación en $\mathbb{Q}[t]$ tenga solución entera. Se establece además una fórmula para las soluciones de las ecuaciones de grado hasta 1.

No obstante, en el transcurso de la investigación he comprobado que al menos existen estos otros problemas relacionados aún abiertos:

a. No se han probado las tres desigualdades simultáneas del teorema de Holzer en $\mathbb{Z}[i]$. Lo he intentado sin éxito.

b. No se conocen cotas para los coeficientes enteros de las soluciones en $\mathbb{Q}[t]$.

c. Existen otros dominios euclídeos de características parecidas a los enteros de Gauss, dominios cuadráticos imaginarios tales como $\mathbb{Z}[\sqrt{-2}]$, $\mathbb{Z}[\sqrt{-3}]$, $\mathbb{Z}[\sqrt{-7}]$, $\mathbb{Z}[\sqrt{-11}]$, para los cuales no se han generalizado cotas de Holzer.

d. No se han probado cotas del tipo de Holzer para las soluciones enteras de la ecuación cuadrática general

$$ax^2 + bxy + cy^2 + dxz + eyz + fz^2 = 0.$$

Yo conjeturo que existe una solución (x, y, z) que de forma simultánea satisface

$$|x| < \sqrt{|e^2 - 4cf|}, \quad |y| < \sqrt{|d^2 - 4af|}, \quad |z| < \sqrt{|b^2 - 4ac|},$$

pero al intentar probarlo por los mismos procedimiento descritos en esta tesis, tropiezo con una dificultad que no he podido resolver.

e. También en los Cuaterniones, de característica distinta es el dominio euclídeo $\mathbb{H}$ de los Cuaterniones de Hurtwitz,

$$\mathbb{H} = \{a + bi + cj + dk : a, b, c, d \in \mathbb{Z} \quad \text{ó} \quad a, b, c, d \in \mathbb{Z} + \frac{1}{2}\}$$

donde

$$\mathbb{Z} + \frac{1}{2} := \{n + \frac{1}{2}, n \in \mathbb{Z}\}$$

Este anillo es un anillo de división, no es conmutativo para el producto y se tendría que considerar ecuaciones de Legendre por la derecha y por la izquierda.

f. En los Octoniones, un dominio mucho más complejo y no muy estudiado es el anillo euclídeo de los Octaviones ...

Bibliography

[1] J. L. Lagrange, *Sur la solution des problèmes indéterminés du second degré*, Hist. Ac. Berlin, anné 1767 (t. 23), pp. 165-310; Œuvres complètes, tome II, pp. 539-578.

[2] M. Legendre, *Théorème sur la possibilité des équations indeterminées du second degré*, Histoire de l'Acadmie Royale des Sciences, (1785), pp. 507-513.

[3] K. F. Gauss, *Solutio aequationis* $axx + byy + czz = 0$, Disquisitiones Arithmeticae (1801), art. 294.

[4] K. F. Gauss, *Le Gendre theorema fundamentale tractauit*, Disquisitiones Arithmeticae (1801), art. 296.

[5] M. Legendre, *Théorie de Nombre.* Chez Firmin Didot Frères, Libraires. Troisième édition (1830), pp. 32-40.

[6] P.G. Lejeune Dirichlet, R. Dedekind *Vorlesungen uber Zahlentheorie* (1871) art. 156-157, pp. 408-421.

[7] M. S. Réalis, *Note sur quelques équations indéterminées* Nouvelle Correspondance Mathématique (1878), pp. 369-371.

[8] L. E. Dickson, *History of the Theory of Numbers. Volume II. Diophantine Analysis*, Carnegie Institute of Washington No 256 (1919), pp. 419-428.

[9] H. Hasse, *Uber die Darstellbarkeit von Zahlen durch quadratische Formen im Krper der rationalen Zahlen* J. reine angew. Math., **152** (1923), 129-148; 205-224.

[10] L. E. Dickson, *Modern Elementary Theory of Numbers*, Chicago (1939), pp. 155-159.

[11] H. Davenport and Marshall Hall, *On the equation* $ax^2 + by^2 + cz^2 = 0$, Quaterly journal of Mathematics Oxford Series. Vol. **19** (1948), pp. 189-192.

[12] L. Holzer, *Minimal solutions of diophantine equations*, Can. J. Math. **2** (1950), 238-244.

[13] L. J. Mordell, *On the Equation* $ax^2 + by^2 - cz^2 = 0$., Monatshefte für Math. 53 (1951), pp. 323-327.

[14] Trygve Nagell, *Introduction to Number Theory* , Uppsala (1951), §61, pp 218-222.

[15] P. A. Samet, *An equation in gaussian integers*, The American Mathematical monthly Vol. **59**, No 7 (1952), pp. 448-452.

[16] Ove Hemer, *On the solvability of the diophantine equation* $ax^2 + by^2 + cz^2 = 0$ *in imaginary Euclidean quadratic fields*, Arkiv for Matematik Vol. **2**, No 2 (1951), pp. 57-82.

[17] Robert Spira, *The Diophantine Equation* $x^2+y^2+z^2 = m^2$, The American Mathematical Monthly Vol. **69**, No. 5 (May, 1962), pp. 360-365

[18] L. J. Mordell, *On the Magnitude of the Integer Solutions of the Equation* $ax^2 + by^2 + cz^2 = 0$, Journal of Number Theory **1** (1969), pp. 1-3.

[19] L. J. Mordell, *Diophantine Equations*, Academic Press (1969), pp. 43-45.

[20] L. J. Mordell, *Diophantine Equations*, Academic Press (1969), pp. 31.

[21] I. Niven, H.S. Zuckerman, H.L. Montgomery, *An introduction to the Theory of Numbers*, John Wiley & Sons, Fifth Edition (1991), pp. 242-245.

[22] Hans Liebeck; Anthony Osborne, *the Generation of All Rational Orthogonal Matrices* , The American Mathematical Monthly, Vol. 98, No. 2. (Feb., 1991), pp. 131-133.

[23] T. Cochrane y P. Mitchell, *Small solutions of the Legendre equation*, Journal of Number Theory **70**(1) (1998), pp. 62-66.

[24] Zhiming M. OU, Kenneth S. Williams, *Small solutions of* $\phi_1 x_1^2 + \cdots + \phi_n x_n^2 = 0$, Canad. J. Math. Vol. **52** (3), (2000) pp. 613-632.

[25] J. E. Cremona and D.Rusin, *Efficient solution of rational conics*, Mathematics Of Computation Vol. **72**, No. 243, (2002) pp. 1417-1441.

[26] Po-Ju. Shih, *Legendre's Theorem in $Z[i]$ and in $Z[\omega]$*. National Central University Library Electronic theses and Dissertations System. (2004)

[27] Laura M. Nunley, *Geometry of Numbers Aprroach to Small Solutions to the Extended Legendre Equation*, Thesis. Electronic Version. University of Georgia. Athens, Georgia. (2010)

[28] Sophie Frisch, Leonid Vaserstein, *Polynomial parametyrization of Pythagorean quadruples, quintuples and sextuples*, Journal of Pure and applied Algebra No 216 (2012), pp. 184-191.

[29] J. L. Leal-Ruperto, *On the magnitude of the Gaussian integer solutions of the Legendre equation*, Journal of Number Theory No 145 (2014), pp. 572-578.

[30] J. L. Leal-Ruperto, *On the solvability of Legendre equation in the rational polynomial ring $\mathbb{Q}[t]$*, aceptado en revisión en Journal of Number Theory.

[31] J. L. Leal-Ruperto, *On the magnitude of the rational polynomial solutions of the Legendre equation*, Enviado para su posible publicación a Journal of Number Theory.